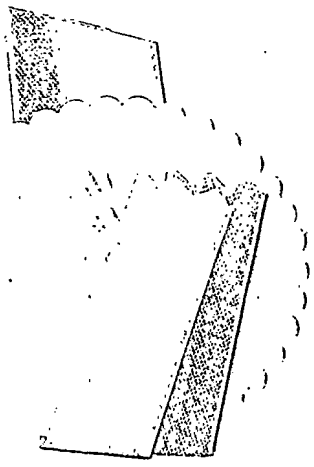
日本国特許庁 30. 1. 2004
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　１月３１日

出願番号
Application Number: 特願２００３－０２４１６７
[ST. 10/C]: [ＪＰ２００３－０２４１６７]

出願人
Applicant(s): 松下電器産業株式会社



２００４年　３月１２日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００４－３０１９５４６

【書類名】　特許願

【整理番号】　2968240067

【提出日】　平成15年 1月31日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 12/00542

G06K 19/07

【発明者】

【住所又は居所】　東広島市鏡山３丁目１０番１８号　株式会社松下電器情報システム広島研究所内

【氏名】　江原　裕美

【発明者】

【住所又は居所】　東広島市鏡山３丁目１０番１８号　株式会社松下電器情報システム広島研究所内

【氏名】　川野　眞二

【発明者】

【住所又は居所】　東広島市鏡山３丁目１０番１８号　株式会社松下電器情報システム広島研究所内

【氏名】　中部　太志

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100090446

【弁理士】

【氏名又は名称】　中島　司朗

【手数料の表示】

【予納台帳番号】　014823

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9003742

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　半導体メモリカード、コンピュータ読み取り可能なプログラム

。

【特許請求の範囲】

【請求項１】　耐タンパモジュールと、不揮発メモリとを備える半導体メモリカードであって、

耐タンパモジュールは、内部メモリと、処理部とを含み、

耐タンパモジュールの内部メモリには、アプリケーションプログラムにより利用される領域があり、

前記処理部は、

当該アプリケーションプログラムに固有のファイルシステム領域を不揮発メモリ上に割り当て、当該ファイルシステム領域についてのアクセステーブルを耐タンパモジュールの内部メモリ上に配置することにより、アプリケーションプログラムの利用領域の拡張を行う

ことを特徴とする半導体メモリカード。

【請求項２】　前記処理部は、

使用領域の拡張にあたって、拡張領域を利用するアプリケーションプログラムに固有の暗号鍵を割り当て(1)、

アプリケーションプログラムが前記拡張領域にデータを書き込もうとする際、当該データを暗号化し(2)、

アプリケーションプログラムが当該拡張領域からデータを読み出そうとする際、当該データを復号化する(3)暗復号化部を備える

ことを特徴とする請求項１記載の半導体メモリカード。

【請求項３】　前記処理部は、アプリケーションプログラムからセキュリティレベルを受け付ける受付部と、

セキュリティレベルがとり得る複数の値と、それらの値に対応する暗号鍵のビット長、暗号方式を記憶する記憶部とを備え、

前記暗復号化部により割り当てられる暗号鍵は、

受付手段が受け付けたセキュリティレベルに対応するビット長に基づき生成さ

れ、

前記暗復号化部による暗号化及び復号化は、

受付手段が受け付けたセキュリティレベルに対応する暗号方式に基づきなされる

ことを特徴とする請求項２記載の半導体メモリカード。

【請求項４】　前記暗復号化部は、

ファイルシステム領域とは異なる暗号鍵をアクセステーブルに割り当てて、その暗号鍵で、アクセステーブルを暗号化した上で耐タンパモジュールの内部メモリ上に配置する

ことを特徴とする請求項３記載の半導体メモリカード。

【請求項５】　前記処理部は、別のアプリケーションプログラムの利用領域の拡張を、

不揮発メモリ上に別のアプリケーションプログラムについてのファイルシステム領域を割り当て、同不揮発メモリ上に当該ファイルシステム領域についてのアクセステーブルを配置することにより行い、

前記暗復号化部は、

ファイルシステム領域とは異なる暗号鍵をアクセステーブルに割り当てて、その暗号鍵で、アクセステーブルを暗号化した上で不揮発メモリ上に配置する

ことを特徴とする請求項３記載の半導体メモリカード。

【請求項６】　耐タンパモジュールと、不揮発メモリとを備える半導体メモリカードであって、

耐タンパモジュールは、内部メモリと、処理部とを含み、

耐タンパモジュールの内部メモリには、アプリケーションプログラムにより利用される領域があり、

前記処理部は、

当該アプリケーションプログラムに固有のファイルシステム領域と、当該ファイルシステム領域についてのアクセステーブルとを不揮発メモリ上に配置し(1)、

これらファイルシステム領域及びアクセステーブルのそれぞれに相異なる暗号

鍵を割り当て(2)、

それら相異なる暗号鍵を耐タンパモジュールの内部メモリ上に配置することにより、アプリケーションプログラムの利用領域の拡張を行う(3)

ことを特徴とする半導体メモリカード。

【請求項７】　耐タンパモジュールと、不揮発メモリとを備える半導体メモリカードにおいて、耐タンパモジュール内のＣＰＵにより実行されるコンピュータ読取可能なプログラムであって、

耐タンパモジュールは、内部メモリを含み、

耐タンパモジュールの内部メモリには、アプリケーションプログラムにより利用される領域があり、

当該アプリケーションプログラムに固有のファイルシステム領域を不揮発メモリ上に割り当て、当該ファイルシステム領域についてのアクセステーブルを耐タンパモジュールの内部メモリ上に配置することにより、アプリケーションプログラムの利用領域の拡張する手順をＣＰＵに行わせる

ことを特徴とするコンピュータ読取可能なプログラム。

【請求項８】　前記コンピュータ読取可能なプログラムは、

使用領域の拡張にあたって、拡張領域を利用するアプリケーションプログラムに固有の暗号鍵を割り当て(1)、

アプリケーションプログラムが前記拡張領域にデータを書き込もうとする際、当該データを暗号化し(2)、

アプリケーションプログラムが当該拡張領域からデータを読み出そうとする際、当該データを復号化する(3)手順をＣＰＵに行わせる

ことを特徴とする請求項７記載のコンピュータ読取可能なプログラム。

【請求項９】　前記コンピュータ読取可能なプログラムは、アプリケーションプログラムからセキュリティレベルを受け付ける受付ステップをＣＰＵに実行させるものであり、

耐タンパモジュールの内部メモリには、

セキュリティレベルがとり得る複数の値と、それらの値に対応する暗号鍵のビット長、暗号方式を示すテーブルが存在し、

前記暗復号化ステップにより割り当てられる暗号鍵は、

受付手段が受け付けたセキュリティレベルに対応するビット長に基づき生成され、

前記暗復号化ステップによる暗号化及び復号化は、

受付手段が受け付けたセキュリティレベルに対応する暗号方式に基づきなされる

ことを特徴とする請求項８記載のコンピュータ読取可能なプログラム。

【請求項１０】　前記暗復号化ステップは、

ファイルシステム領域とは異なる暗号鍵をアクセステーブルに割り当てて、その暗号鍵で、アクセステーブルを暗号化した上で耐タンパモジュールの内部メモリ上に配置する手順をＣＰＵに行わせる

ことを特徴とする請求項９記載のコンピュータ読取可能なプログラム。

【請求項１１】　前記コンピュータ読取可能なプログラムは、別のアプリケーションプログラムの利用領域の拡張にあたって、

不揮発メモリ上に別のアプリケーションプログラムについてのファイルシステム領域を割り当て、同不揮発メモリ上に当該ファイルシステム領域についてのアクセステーブルを配置する処理をＣＰＵに行わせ、

前記暗復号化ステップは、

ファイルシステム領域とは異なる暗号鍵をアクセステーブルに割り当てて、その暗号鍵で、アクセステーブルを暗号化した上で不揮発メモリ上に配置する手順をＣＰＵに行わせる

ことを特徴とする請求項９記載のコンピュータ読取可能なプログラム。

【請求項１２】　耐タンパモジュールと、不揮発メモリとを備える半導体メモリカードにおいて、耐タンパモジュール内のＣＰＵにより実行されるコンピュータ読取可能なプログラムであって、

耐タンパモジュールは、内部メモリと、処理部とを含み、

耐タンパモジュールの内部メモリには、アプリケーションプログラムにより利用される領域があり、

前記コンピュータ読取可能なプログラムは、

当該アプリケーションプログラムに固有のファイルシステム領域と、当該ファイルシステム領域についてのアクセステーブルとを不揮発メモリ上に配置し(1)、

これらファイルシステム領域及びアクセステーブルのそれぞれに相異なる暗号鍵を割り当て(2)、

それら相異なる暗号鍵を耐タンパモジュールの内部メモリ上に配置することにより、アプリケーションプログラムの利用領域の拡張を行う(3)手順をＣＰＵに行わせる

ことを特徴とするコンピュータ読取可能なプログラム。

【発明の詳細な説明】

【０００１】

【発明が属する技術分野】

本発明は、格納内容のセキュリティを保証した半導体メモリカードに関し、その記憶容量を拡張する技術の改良に関する。

【０００２】

【従来の技術】

半導体メモリカードの生産業は、放送･出版等のマスメディアから金融機関、国、自治体まで、様々な分野からの注目を浴びる近年の急成長産業である。

これらの分野から注目を集めているのは、格納内容の保護機能である。格納内容の保護機能をもった半導体メモリカードの代表格は、SDメモリカード、非接触ICカードである。SDメモリカードは、接触型の半導体メモリカードであり、不揮発メモリと、ロジック回路と、コネクタとを備える、コネクタを介してホスト装置が接続した場合、SDメモリカードはチャレンジ･レスポンス型の相互認証を行い、互いの正当性を認識した上で、ホスト装置による不揮発メモリのアクセスを許可する。不正な機器によるアクセスを排斥することができ、また内蔵している不揮発メモリの規模は、64Mバイト～1Gバイトという大規模なものなので、SDメモリカードは、著作権保護が必要なオーディオデータ、ビデオデータの格納に向いている。

【０００３】

非接触ICカードは、CPU、マスクROM、EEPROMを内蔵したICチップを板体に配してなる。板体には螺旋アンテナが埋設されており、非接触ICカードがこの螺旋アンテナを介して、ホスト装置と非接触型のデータ入出力を行う。またこのICチップは耐タンパモジュールと呼ばれ、分解や解析等のリバース行為に耐性をもつ。

この耐性があるため、非接触ICカードは金銭決済用途に向いており、多くのクレジット会社や金融機関がこの非接触ICカードの採用を検討している。その反面、耐タンパモジュールは、単位面積当たりの製造コストが高く、耐タンパモジュール内のEEPROMの規模は160Kバイト程度である。

【０００４】

このようにSDメモリカード、非接触ICカードには一長一短があり、どちらが優れているがは簡単には結論付けることはできない。

尚、SDメモリカードについての先行技術には、以下の特許文献1に開示されたものがある。

【０００５】

【特許文献1】

特開2001-14441号公報

【０００６】

【発明が解決しようとする課題】

ところで、クレジット会社のサーバ装置をホスト装置とした電子商取引(EC(Electronic Commerce))では、年間の取引明細をダウンロードして、非接触ICカードに格納しておきたいことがある。年間の取引明細となると、データサイズが大きく、非接触ICカードのメモリでは容量に不足が生じる。容量が不足するとはいえ、SDメモリカードのような耐タンパモジュールの無い半導体メモリカードに取引明細を格納しようというのは、クレジット会社にとって不安が残る。何故なら、かかる年間の取引明細は、金銭に至らないまでも、それに準ずる保護価値があるからである。

【０００７】

半導体メモリカードを製造する生産業のメーカは、製造コストの高騰を承知で耐タンパモジュールを大規模するか、或は、クレジット会社の要求を黙殺するか

を選択せざるを得ない。現状では、半導体メモリカードのメーカは苦渋の決断を迫られているといえる。

本発明の目的は、金銭に準ずるデータであってサイズが膨大なものを、相応のセキュリティレベルで格納しておくことができる半導体メモリカードを提供することである。

【０００８】

【課題を解決するための手段】

上記目的を達成するため、本発明に係る半導体メモリカードは、耐タンパモジュールと、不揮発メモリとを備え、耐タンパモジュールは、内部メモリと、処理部とを含み、耐タンパモジュールの内部メモリには、アプリケーションプログラムにより利用される領域があり、　前記処理部は、当該アプリケーションプログラムに固有のファイルシステム領域を不揮発メモリ上に割り当て、当該ファイルシステム領域についてのアクセステーブルを耐タンパモジュールの内部メモリ上に配置することにより、アプリケーションプログラムの利用領域の拡張を行うことを特徴としている。

【０００９】

【発明の実施の形態】

以降、本発明に係る半導体メモリカードの実施形態について説明する。本実施形態に係る半導体メモリカードは、非接触ICカードの耐タンパモジュールを内蔵したSDeXメモリカードである。SDeXメモリカードは、SDメモリカード同様、SDポータブルデバイスの記録媒体に用いられながらも、非接触ICカードの耐タンパモジュールを内蔵している。

【００１０】

先ず始めに、本発明に係る半導体メモリカード(SDeXメモリカード)の実施行為のうち、使用行為について説明する。SDeXメモリカードは、携帯電話などのSDポータブルデバイスと接続され、図１に示すような環境で、ユーザの利用に供される。図１は、SDeXメモリカードの使用環境を示す図である。

図１における使用環境は、ECサーバ１００、カードリーダライタ２００、無線基地局２１０、SDポータブルデバイス３００から構成される。

【００１１】

ECサーバ１００は、カードリーダライタ２００及び無線基地局１００、ネットワークを介して、非接触ICカードにECサービスを提供する。ECサーバ１００には複数のECアプリケーションプログラムが動作しており、これらのそれぞれは、固有のECサービスを非接触ICカードに提供する。ECサーバ１００上で動作するECアプリケーションは、サーバアプリケーションであり、ECサービスの種類毎にそれぞれ違うものが存在する。図１では、n種のECサービス毎のECアプリをS_APL1,2,3・・・nと略記している。これらは、n種のサーバアプリケーションである。ECサーバ１００によるECサービス提供は、ネットワーク、カードリーダライタ２００及び無線基地局２１０を介してECコマンドを非接触ICカードに発行することによりなされる。

【００１２】

カードリーダライタ２００は、クレジット会社･金融機関のキャッシュデスペンサー、店舗のレジ機に備え付けの機器であり、非接触ICカードへの電力供給、非接触ICカードとの非接触型の入出力を行う。カードリーダライタ２００は、ネットワークと接続されており、このカードリーダライタ２００を介することで、非接触ICカードはECサーバ１００のECサービスを受けることができる。

【００１３】

無線基地局２１０は、建造物や電柱の屋上に備え付けの機器であり、携帯電話型のSDポータブルデバイス３００と無線によるデータの入出力を行う。無線基地局２１０は、ネットワークと接続されており、この無線基地局２１０を介することでも、SDポータブルデバイス３００はECサーバ１００のECサービスを受けることができる。

【００１４】

SDポータブルデバイス３００は、SDeXメモリカードを接続して、SDeXメモリカードをアクセスする機器である。SDポータブルデバイス３００には、ブラウザソフト等がインストールされており、ユーザはこのブラウザのユーザインターフェイスを介して、SDeXメモリカードにおけるファイルシステム(File System(以下、FSと略す場合がある))をアクセスすることができる。このファイルシステムア

クセスは、SDメモリカードで規定されているSDコマンドをSDeXメモリカードに発行し、そのレスポンスをSDeXメモリカードから受信することでなされる。また、SDポータブルデバイス３００がSDeXメモリカードからブートストラップを行って起動する場合、SDポータブルデバイス３００はSDeXメモリカードと一体になって非接触ICカードとして機能する。SDポータブルデバイス３００の背面には、螺旋アンテナが埋設されており、非接触ICカードとしての機能時において、この螺旋アンテナが、カードリーダライタ２００から発せられる電力をSDeXメモリカードに供給する。またSDポータブルデバイス３００は、SDeXメモリカードに対するコマンド･レスポンスと、ECサーバ１００とのコマンド･レスポンスとの相互変換を行う。SDポータブルデバイス３００による相互変換とは、ECサーバ１００からのECコマンドをカプセル化した拡張SDコマンドを生成してSDeXメモリカードに出力し、SDeXメモリカードからのSDレスポンスよりECレスポンスを取り出して、ECサーバ１００に出力する処理である。SDポータブルデバイス３００がSDeXメモリカードにてブートストラップを行い、非接触ICカードとして機能することを『ECモード』という。また、SDポータブルデバイス３００がSDeXメモリカードを記録体として用いることを『SDモード』という。

【００１５】

SDモードでのSDeXメモリカードの利用は、SDeXメモリカード本来の用途である。この用途においてSDeXメモリカードのホスト装置となるのは、SDポータブルデバイス３００であり、ホスト装置であるSDポータブルデバイス３００が配信サーバからダウンロードしたオーディオデータ、ビデオデータの受け皿として、SDeXメモリカードは用いられる。こうしてSDeXメモリカードに記録されたオーディオデータ、ビデオデータをホスト装置は再生させることができる。

【００１６】

ECモードでのSDeXメモリカードの利用は、非接触ICカードの用途である。このECモードにおいてもSDeXメモリカードはSDポータブルデバイス３００と接続される。しかしSDeXメモリカードのホスト装置となるのはこのSDポータブルデバイス３００ではなく、ネットワーク上のECサーバ１００である。SDeXメモリカードと接続されたSDポータブルデバイス３００を、カードリーダライタ２００、無線基

地局２１０と用いることにより、SDeXメモリカードはECサーバ１００と通信を行う。この通信により、ECサーバ１００と金銭決済を行うことができる。

【００１７】

本実施形態のSDeXメモリカードは、配信されたオーディオデータ、ビデオデータの受け皿としても用途に加え、非接触ICカードとしても用途が存在するので、ユーザにとっての利便性が増している。

尚図１においてSDeXメモリカードは、SDモードにおいてカードリーダライタ２００を介して、ECサーバ１００をアクセスしたが、無線基地局２１０を介してSDポータブルデバイス３００がネットワークを介してECサーバ１００をアクセスしてもよい。

【００１８】

続いて本発明にかかる半導体メモリカードの生産行為の形態について説明する。本発明に係る半導体メモリカードは、図２、図３の内部構成に基づいて工業的に生産することができる。

図２に示すように、本発明にかかる半導体メモリカードの内部には、コネクタ、耐タンパ性を有する耐タンパモジュールチップ(Tamper Resist Module(TRM))１、256Mバイトもの容量をもつEEPROMチップ(図中のEEPROM)２が実装されている。

【００１９】

耐タンパ性には、諸説があるが、概して以下のことを意味するとされている。

①チップを物理的に開梱しても、内部構成は判読不可能である。

②電磁波を照射しても内部構成は判読不可能である。

③入力データのデータ長と、処理時間との関係がノンリニアである。

④入力データによりエラーが発生した際の処理結果により、出力データが逆算されない。

【００２０】

これら①～④の性質をもつため、TRM１は多くのリバース行為に耐性をもつ。以降、TRM１内のハードウェア要素について説明する。

図３は、TRM１内のハードウェア構成を示す図である。図３に示すようにTRM１

には、内部EEPROM３、外部メモリ制御部４、HIM５、マスクROM６、CPU７が実装されており、マイコンシステムを形成している。

【００２１】

内部EEPROM３は、読み出し／書き込みが可能なメモリである。TRM１として実装されたマイコンシステムは、単位面積当たりの製造コストが高く、TRM１内の内部EEPROM３の規模は、32Kバイトになっている。この内部EEPROM３と区別するため、図２に示したEEPROMを、以降外部EEPROM２と呼ぶ。

外部メモリ制御部４は、外部EEPROM２のアクセスのために設けられた専用回路である。外部EEPROM２のアクセスは、SDポータブルデバイス３００が発するSDコマンドに基づき行われる。

【００２２】

HIM(Host Interface Module)５は、SDポータブルデバイス３００から発行されるSDコマンドのコマンド番号を参照し、そのコマンド番号によりSDコマンドの振り分けを行う。SDコマンドの番号には、1～mの数値と、m+1以上の拡張番号とがある。番号が1～mなら外部メモリ制御部４にSDコマンドを出力し、m+1以上ならSDコマンドにカプセル化されたECコマンドを取り出して、CPU７側へと出力する。

【００２３】

マスクROM６は、OS(Operation System)、Java（登録商標）仮想マシン、アプリケーションプログラムが予め格納されている読出専用メモリである。SDポータブルデバイス３００は、このマスクROM６の固定番地からブートストラップを行うことにより、ECモードとして起動する。

CPU７は、マスクROM６に格納されているプログラムを実行する。

【００２４】

図４は、図３のTRM１内のマスクROM６とCPU７とからなる部分を、ソフトウェア構成に置き換えて描いた図である。破線枠wk1内は、非接触ICカードと互換性があるモジュールである。一方TRM１において破線枠外の部分は、SDメモリカードと互換性があるモジュールである。

SDメモリカードとの互換部分は、外部メモリ制御部４と、HIM５とからなる。この中でHIM５は、SDメモリカードにおける機能を踏襲しつつも、非接触ICカー

ド互換モジュールとの窓口としての機能を果たす。

【００２５】

非接触ICカード互換モジュールは、レイア構造をもつ。このレイヤ構造では、最下位層(物理層)に内部EEPROM３があり、この内部EEPROM３の上位層にOS１０が、更に上位層にはJava（登録商標）仮想マシン９が、最上位層にはECクライアントアプリ８がある。SDメモリカードとの互換部分である外部メモリ制御部４は、内部EEPROM３と同じく物理層にあることは注意されたい。

【００２６】

以降、図４に示したソフトウェア構成(ECクライアントアプリ８、Java（登録商標）仮想マシン９、OS１０)について説明する。

クライアントアプリ８は、ECクライアントアプリ８はJava（登録商標）言語で記述されたECアプリの一種であり、ユーザの操作に基づきECサーバ１００をアクセスする。ECサーバ１００におけるサーバアプリは、ECサービス毎の複数種類のものが存在するので、SDeXメモリカードにおけるクライアントアプリも、ECサービス毎の複数のものが存在する。図中のC_APL1,2,3‥‥nは、ECサーバ１００におけるサーバアプリS_APL1,2,3‥‥nのそれぞれについて、クライアントアプリが存在することを示す。クライアントアプリ８がカードリーダライタ２００、無線基地局２１０やネットワークを介して、ECサーバ１００上のECアプリとコマンドの送受信を行うことにより、ECにおける様々なECサービスを享受する。ECアプリから受信したECコマンドがデータの書き込みコマンドである場合、クライアントアプリは、そのECコマンドをJava（登録商標）仮想マシンを介してOS１０に出力する。

【００２７】

クライアントアプリ本来の役割の他に、ECクライアントアプリ８は、ユーザ操作に基づく外部EEPROM２及び内部EEPROM３のアクセスをECモードにおいて実行する。このアクセスにはファイルをクリエイトしたり、そのファイルを読み書きしたりするというファイルアクセスが含まれる。

Java（登録商標）仮想マシン９(図中のJava(登録商標)Card VM)は、Java（登録商標）言語で記述されたECクライアントアプリ８を、CPU７のネイティブコー

ドに変換して、CPU７に実行させる。

【００２８】

OS１０は、クライアントアプリが発行したコマンドに基づく外部EEPROM２及び内部EEPROM３の読み書きを実行する。以上が、SDeXメモリカードのソフトウェア構成である。

続いて外部EEPROM２及び内部EEPROM３における論理フォーマットについて説明する。図５は、外部EEPROM２及び内部EEPROM３の論理フォーマットを示す図である。外部EEPROM２及び内部EEPROM３は、2つのメモリ空間sm1,sm2を構成している。メモリ空間sm1は、TRM１内のCPU７からアクセス可能なメモリ空間であり、ECアプリの使用領域２１、セキュア領域２２からなる。メモリ空間sm2は、TRM１内CPU７を介することなく、SDポータブルデバイス３００がアクセスすることができるメモリ空間であり、認証領域２３と、非認証領域２４とがある。認証領域２３、非認証領域２４とは、SDメモリカードがもつメモリ領域であり、その意味合いについては上述した特許文献1(特開2001-14441号公報)を参照されたい。

【００２９】

図６は、セキュア領域２２、認証領域２３、非認証領域２４の内部を示す図である。セキュア領域２２、認証領域２３、非認証領域２４は、ISO/IEC 9293に準拠したファイルシステム構造を有する。ISO/IEC 9293は、説明の便宜のために選んだファイルシステム構造の一例に過ぎず、UDF(Universal Disk Format)等、他のファイルシステム構造を有していてもよい。

【００３０】

セキュア領域２２は、TRM１内のECアプリの使用領域の拡張領域であり、内部EEPROM３上の領域２２aと、外部EEPROM２上の領域２２bとからなる。外部EEPROM２上の領域２２bには、ファイルシステム領域であるパーティション1,2,3・・・・nが存在する。本発明にいう『ファイルシステム領域』は、このパーティションに対応する。一方マスタブートレコードやパーティションへのアクセステーブル(パーティションテーブル1,2,3・・・・n)は、内部EEPROM３内の領域２２a上にある。

【００３１】

SDモードにおいてSDポータブルデバイス３００がアクセスできるのは、TRM１

外の外部EEPROM２のみであり、TRM１内のEEPROM３はアクセスすることができない。この内部EEPROM３内にマスタブートレコードやパーティションテーブルが存在するので、SDポータブルデバイス３００はセキュア領域２２内のパーティション1,2,3‥‥nを認識することができない。SDポータブルデバイス３００により認識されるのは、マスタブートレコードやパーティションテーブルが外部EEPROM２内にある認証領域２３、非認証領域２４に限られる。

【００３２】

CPU７によるセキュア領域２２のアクセスは、CPU７からのアクセス時、つまりECモードでないとなし得ない。このことから外部EEPROM２、内部EEPROM３を跨いで存在するセキュア領域２２のアクセスは、ECモードに限られることがわかる。

セキュア領域２２内のパーティションや、認証領域２３のパーティション、非認証領域２４のパーティションは、共通の内部構成を有する。図７は、パーティションの共通構成を示す図である。

【００３３】

パーティションは、パーティションブートセクタ、『二重化ファイルアロケーションテーブル』、『ルートディレクトリエントリ』、ユーザデータ領域からなる。

『パーティションブートセクタ』は、パーティションに関する情報が記述されたテーブルである。

【００３４】

『二重化ファイルアロケーションテーブル(File Allocation Table(FAT))』は、ISO/IEC 9293に準拠した2つのFATからなる。各FATは、各クラスタに対応づけられた複数のFATエントリーからなる。各FATエントリーは、対応するクラスタが使用中であるか、未使用であるかを示すものであり、対応するクラスタが未使用であれば、そのファイルエントリーには、"0"が設定され、対応するクラスタが使用中であれば、クラスタ番号が設定される。このクラスタ番号は、対応するクラスタが読み出された場合、次にどのクラスタを読み出せばよいかといったクラスタ間のリンク関係を示す。

【００３５】

『ルートディレクトリエントリ』は、ルートディレクトリに存在する複数ファイルについてのファイルエントリーを複数含む。各ファイルエントリーは、存在するファイルの「ファイル名」と、そのファイルの「ファイル拡張子」と、ファイルの先頭部が格納されている「ファイル最初のクラスタ番号」と、そのファイルについての「ファイル属性」と、ファイルが記録された「記録時刻」と、ファイルの「記録日付」と、ファイルのデータ長である「ファイル長」とを含む。

【００３６】

『ユーザ領域』は、ファイルが格納される領域である。以上がパーティションの構成である。続いてパーティションテーブル及びパーティションブートセクタについて説明する。

セキュア領域２２のパーティションテーブルは、内部EEPROM３に存在する。一方認証領域２３、非認証領域２４についてのパーティションテーブルは、外部EEPROM２に存在する点に違いがある。しかし、セキュア領域２２、認証領域２３、非認証領域２４のパーティションテーブルは何れも図８（ａ）の内部を有する。図８（ａ）は、パーティションテーブルを示す図であり、図８（ｂ）は、図７のパーティション内のパーティションブートセクタを示す図である。

【００３７】

『パーティションテーブル』は、図８（ａ）の矢印ky2に示すように、"Boot Indicator"と、パーティションの開始ヘッダを特定する"Starting Head"と、パーティションの開始セクタ･開始シリンダを特定する"Starting Sector/Starting Cylinder"と、ファイルシステムのタイプを示す"SystemID"と、"Ending Head"と、パーティションの終了セクタ･終了シリンダを特定する"Ending Sector/Ending Cylinder"と、このパーティションの開始セクタまでの相対セクタ数を示す"Relative Sector"と、パーティションのセクタ数が設定される"Total Sector"とからなる。

【００３８】

パーティションブートセクタは、図８（ｂ）に示すような情報項目を有するExtend FDC記述子が設定される。図８（ｂ）によれば、Extend FDC記述子は、Jump Command,Creating System Identifier,一セクタのサイズ(Sector Size)，一ク

ラスタ当たりのセクタ数(Sector per Cluster),Reserved Sector Count,二重化FATに含まれるFAT数(Numbr of FATs),ルートディレクトリエントリのデータ長(Number of Root-directory Entries),Total Sectors,Medium Identifier,FAT1つ当たりのセクタ数(Sector Per FAT),Sector Per Track,Number of Sides,Number of Hidden Sectors,総セクタ数(Total Sectors),Physical Disk Number,Extended Boot Record Signature,Volume ID Number,ボリュームラベル(Volume Label),File System Type,Signature Word等の項目が設定される。

【００３９】

以上が、TRM１の内部構成である。続いて、領域拡張部１１について説明する。以下、この領域拡張部１１を設けたことの技術的意義を説明する。

非接触ICカード互換モジュールにおいて、ECアプリから受信したデータは、内部EEPROM３に書き込まれる。ECアプリから書き込みが要求されるデータは、金銭に係るものであり、大半がサイズが小さく内部EEPROM３でも充分収まる。ところが年間の取り引き明細に関するデータ書き込みがECアプリから要求された場合、サイズが余りにも大きく内部EEPROM３の容量では不足が生ずる。だからといってかかるデータを外部EEPROM２にそのまま書き込むのは、セキュリティ上好ましくない。何故なら、かかる年間の取引明細は、金銭に至らないまでも、それに準ずる保護価値があるからである。

【００４０】

そこで領域拡張部１１は、TRM１に準ずるセキュリティを保証しつつ、ECアプリの使用領域を、内部EEPROM３から外部EEPROM２へと拡張する。

領域拡張部１１は、ECアプリのECアプリの使用領域の拡張にあたって、ECアプリに外部EEPROM２内の1つのファイルシステムを割り当てる。ECアプリに割り当てられたファイルシステムは、そのECアプリ固有のものであり、他のECアプリはこのファイルシステムをアクセスすることはできない。1つのファイルシステム内部という閉じた空間にて、ECアプリは自由にファイルアクセスを行うことができる。領域拡張部１１により割り当てられるファイルシステムとは、上述したセキュア領域内のパーティションである。領域拡張部１１によるアタッチは、クライアントアプリがファイルシステムOPENを要求した際になされる。ファイルシス

テムOPENが要求された際、領域拡張部１１は外部EEPROM２内に1つのパーティションを生成し、そのパーティションについてのパーティションテーブルを配置する。そしてECアプリには、ファイルシステムを利用するためのAPL-IDを付与する。このAPL-IDは、10桁以上のランダムな数値からなり、パスワードのように用いられる。

【００４１】

領域拡張部１１から付与されたこのAPL-IDを利用することで、ECアプリは自身に割り当てられたファイルシステムにデータを書き込んだり、データを読み出したりすることができる。ファイルシステムのOPENは、いわゆるファイルオープンとは異なる。従ってECアプリがセキュア領域２２のファイルをオープンするには、前もってファイルシステムをOPENし、その後、ファイルをOPENするという二段階のOPENを行わねばならない。

【００４２】

ECアプリによるデータ読み書きが終われば、ファイルシステムのデタッチを行う。ファイルシステムのデタッチとは、ECアプリに割り当てられたパーティションを解放することである。領域拡張部１１によるデタッチは、クライアントアプリがファイルシステムCLOSEを要求した際になされる。ファイルシステムCLOSEが要求された際、デタッチは、領域拡張部１１によりなされる。ファイルシステムのCLOSEも、いわゆるファイルCLOSEとは異なる。ECアプリがセキュア領域２２のファイルをCLOSEした後に、その後、ファイルが存在するファイルシステムをCLOSEするという二段階のCLOSEを行わねばならない。以降、同じECアプリが、同じパーティションを利用するには、APL-IDにより自己の正当性を証明した上で、領域拡張部１１にアタッチを行わせねばならない。

【００４３】

図９は、ECサーバ１００によるSDeXメモリカードのアクセス、SDポータブルデバイス３００によるSDeXメモリカードのアクセスを示す図である。図中の実線の矢印jt1, jt2, jt3は、ECサーバ１００によるSDeXメモリカードのアクセスを模式的に示す。図中の破線の矢印hs1は、SDポータブルデバイス３００によるSDeXメモリカードのアクセスを模式的に示す。本図に示すように、ECアクセスは、内部

EEPROM３、外部EEPROM２内のセキュア領域２２の何れかにアクセス可能であり、ECサーバ１００内のECアプリは、書き込むべきデータの大きさや重要度に応じて、書込先を選ぶことができる。

【００４４】

図１０は、SDeXメモリカード、SDポータブルデバイス３００、ECサーバ１００間におけるコマンド･レスポンスのシーケンス図である。本図において右向きの矢印はコマンドを示し、左向きの矢印は、レスポンスを示す。

SDモードでは、SDポータブルデバイス３００がホスト装置であり、SDポータブルデバイス３００はHIM５を介してSDeXメモリカードの外部メモリ制御部４と、SDコマンド、SDレスポンスの送受信sc1,2,3,4を行う。

【００４５】

ECモードにおけるシーケンスは、このSDモードにおけるシーケンスを踏襲しつつも、これを応用したものになっている。ECモードにおいても、SDモード同様HIM５を介した外部メモリ制御部４とのコマンド･レスポンスの送受信sc5,6が行われる。これらのコマンド･レスポンスは、ECコマンドをカプセル化したSDコマンド、ECレスポンスをカプセル化したSDレスポンスであり、SDポータブルデバイス３００は、HIM５を介したコマンド･レスポンスの送受信に加え、カードリーダライタ２００、無線基地局２１０、ネットワークを介したECサーバ１００とのECコマンド、ECレスポンスの送受信sc7,8を行う。ECコマンド、ECレスポンスの送受信sc5,6を行う点が、第１の差違点である。ECサーバ１００との送受信において、SDポータブルデバイス３００はその内部で、ECコマンド･ECレスポンスと、SDコマンド、SDレスポンスとの相互変換を行う。

【００４６】

SDモードとの第２の差違は、SDモードにおいてコマンド･レスポンスは外部メモリ制御部４－HIM５をダイレクトに行き来する。これに対し、ECモードではコマンド･レスポンスが非接触ICカード互換モジュールのクライアントアプリ８、領域拡張部１１を経由する点、つまりクライアントアプリ８、領域拡張部１１を通る。この迂回部分uc1,2,3,4,5,6,7が存在する点が第２の差違点である。

【００４７】

迂回部分において、外部EEPROM２への書き込みに先立ち、クライアントアプリは、ファイルシステムのOPEN、ファイルOPENを順次行う。ファイルシステムのOPENが命じられれば領域拡張部１１は、ファイルシステムのアタッチを行う。

一方外部EEPROM２の書き込み後、クライアントアプリは、ファイルのCLOSE、ファイルシステムのCLOSEを行う。ファイルのCLOSEが命じられれば領域拡張部１１は、ファイルシステムのデタッチを行う。

【００４８】

以上のように本実施形態によれば、TRM１の内部EEPROM３から外部EEPROM２へとECアプリの使用領域を拡張するにあたって、ECアプリの使用領域の拡張部にあたるパーティションを外部EEPROM２内に配置しつつも、パーティションテーブルをTRM１内部に置く。拡張部の根幹であるパーティションテーブルをTRM１内に秘匿するので、ECアプリの使用領域の拡張部がどこから始まるかを悪意をもったものに知られずに済む。これにより、ECアプリにより書き込まれたデータの守秘性を保つことができる。

【００４９】

また、ECアプリのそれぞれにパーティションを割り当て、各パーティションの関係を排他的なものにするので、複数ECアプリのうち1つが、悪意をもったものが操作されたとしても、他のECアプリに割り当てられたパーティションの格納内容が、そのECアプリに知られることはない。1つのECアプリによる不正アクセスを、他のECアプリに波及させないので、格納内容の守秘性を保つことができる。

【００５０】

（第２実施形態）

第２実施形態は、第１実施形態より強固に、セキュア領域２２の格納内容を保護する改良に関する。SDeXメモリカードの格納内容の保護は、一般に格納内容を暗号化することで実現される。

しかし不正なECアプリによりセキュア領域２２がアクセスされる場合、セキュア領域２２の格納内容を暗号化する暗号鍵が、そのECアプリを操作する者により暴露される恐れがある。そうした場合、セキュア領域２２をアクセスする他のECアプリの格納内容までも、暴露される恐れがあり、セキュア領域２２をアクセス

する他のECアプリのECプロバイダに損害が波及する。

【００５１】

セキュア領域２２の格納内容の全暴露を避けるべく、本実施形態ではパーティションを各ECアプリに割り当てる際、OS１０は固有の暗号鍵をECアプリに割り当てる。そして各ECアプリが、自身のセキュア領域上のファイルシステムをアクセスする際、ファイルシステムに書き込まれるべきデータ、ファイルシステムから読み出されるべきデータを固有の暗号鍵で暗号化･復号化する。各ECアプリにパーティションを割り当てることに加え、固有の暗号鍵で暗号化･復号化を行うので、たとえ1つのECアプリを操作するユーザが自身に割り当てられた暗号鍵をつきとめたとしても、他のECアプリに対応する暗号鍵が暴露されることはない。

【００５２】

以上の暗号化･復号化を行うため、OS１０は、図１１に示す構成をもつ。図１１に示すようにOS１０は、第１実施形態に示した領域拡張部１１に加え、選択テーブル１２、暗号化テーブル１３、暗復号化部１４を有する。

選択テーブル１２は、複数のビット長と、複数の暗号方式とを対応付けたテーブルである。ビット長は、ECアプリに固有の暗号鍵を生成する際、暗号鍵をどれだけのビット長にするかを示す。暗号方式は、その暗号鍵をもって、どのような暗号化アルゴリズムで暗号化するかを示す。これら複数の暗号方式、ビット長は、１～Lのレベル値があり、高いレベル値には、難易度が高いアルゴリズムの暗号方式と、長いビット長とが対応づけられている。低いレベル値には、難易度が低いアルゴリズムの暗号方式と、短いビット長とが対応づけられている。暗号方式の難易度が高い程、暗号鍵のビット長が長い程、パーティションの格納内容のセキュリティは高くなることを意味する。セキュリティレベルの高低は、暗号化の処理時間と比例関係になる。つまり暗号方式の難易度が高い程、暗号鍵のビット長が長い程、暗号化、復号化に費やされる時間は長くなる。逆に暗号方式の難易度が低い程、暗号鍵のビット長が短い程、パーティションの格納内容のセキュリティは甘くなり、暗号化、復号化に費やされる時間は短くなる。

【００５３】

暗号化テーブル１３は、APL-ID、暗号方式、ビット長の対応をとるテーブルで

ある。

暗復号化部１４は、領域拡張部１１がパーティションをECアプリに割り当てる際、ECクライアントアプリ８からセキュリティレベルを受け取って、選択テーブル１２からそのセキュリティレベルに対応する暗号方式と、ビット長とを選択テーブル１２から検索して(図中のrf1,rf2)、検索したビット長の乱数を発生する。そうして発生した乱数を暗号鍵として固有の暗号鍵をECアプリに割り当てる。この割り当て結果は、暗号化テーブル１３に示される(図中のレコード追加)。以降このECアプリがデータを書き込む際、そのECアプリから受け取ったデータを(図中のWrite data)、割り当てられた暗号鍵を用いてデータを暗号化した上で外部メモリ制御部４に出力する(図中の暗号化Write data)。またECアプリがデータを読み出す際、暗復号化部１４は外部メモリ制御部４から受け取ったデータを(図中の暗号化Read data)そのECアプリに割り当てられた暗号鍵を用いてデータを復号化した上で、ECクライアントアプリ８に引き渡す(Read data)。

【００５４】

第２実施形態に係る領域拡張部１１及び暗復号化部１４は、図１２（ａ）～（ｃ）のフローチャートの処理を行うプログラムをコンピュータ記述言語で記述して、CPU７に実行させることにより生産される。

図１２（ａ）は、領域拡張部１１及び暗復号化部１４の処理手順を示すフローチャートである。

【００５５】

図１２（ａ）のフローチャートにおけるステップＳ１～ステップＳ４は、領域拡張部１１の処理手順を示す。ステップＳ１で、領域拡張の要求元のECアプリに未割当パーティション番号iをアサインし、ステップＳ２では、i番目パーティションについてのパーティションテーブルを内部EEPROM３に書き込み、外部EEPROM２にパーティションを生成する。ステップＳ３において、パスワードを生成し、ステップＳ４では、生成したパスワードをAPL-IDとして要求元アプリに通知する。

【００５６】

また、図１２（ａ）のフローチャートにおけるステップＳ５～ステップＳ７は

、暗復号化部１４の処理手順を示す。ステップＳ５では、拡張要求時のセキュリティレベルに応じた暗号方式、ビット長を選択テーブルから取り出す。ステップＳ６では、取り出されたビット長の乱数を生成し、ステップＳ７では、取り出された暗号方式、ビット長、生成した乱数からなるレコードiを暗号化テーブルに追加する。

【００５７】

図１２（ｂ）は、領域拡張部１１及び暗復号化部１４によるファイル書き込みの処理手順を示すフローチャートである。

ステップＳ１１において、領域拡張部１１は書込を行うアプリに割り当てられたAPL-IDを取得し、ステップＳ１２では、APL-IDからパーティション番号iを特定し、アプリから、パラメータbuf,file,fpの設定を受け付ける。

【００５８】

ここで受け付けられるパラメータには、以下のものがある。

buf:書き込むべきデータへのポインタ

file:書込先ファイルのファイル名

fp:書込先ファイル内部におけるポインタ

ステップＳ１３において暗復号化部１４、buf内のデータを、レコードにおける暗号鍵iを用いて暗号方式iで暗号化し、ステップＳ１４において領域拡張部１１はパーティションiのファイルにおいてファイルポインタ以降に、暗号化データを書き込む。

【００５９】

図１２（ｃ）は、領域拡張部１１及び暗復号化部１４によるファイル読み出しの処理手順を示すフローチャートである。ステップＳ２１において領域拡張部１１は、読出を行うアプリに割り当てられたAPL-IDを取得し、ステップＳ２２において領域拡張部１１は、APL-IDからパーティション番号iを特定する。そしてステップＳ２３において領域拡張部１１は、アプリから、パラメータbuf,file,fp,sizeの設定を受け付ける。

【００６０】

このステップＳ２３で受け付けられるパラメータには、以下のものがある。

buf:読み出すべきデータへのポインタ

file:読出先ファイルのファイル名

fp:読出先ファイル内部におけるポインタ

size:読出データ長

ステップＳ２４において領域拡張部１１はパーティションiのファイルにおいてファイルポインタ以降の暗号化データをsizeだけ読み出し、ステップＳ２５において暗復号化部１４は、暗号鍵iを用いて読み出されたデータを、暗号方式iで復号化して、バッファに格納する。

【００６１】

以上のように本実施形態によれば、ECアプリは、セキュリティレベルと処理時間との関係を考慮して、セキュリティレベルを引数に指定してアタッチをOS１０に要求することができる。これにより、自身がどれだけのセキュリティレベルを要求しているかをOS１０に伝えることができる。

尚、セキュリティレベルはECアプリから受け付けるとしたが、OS１０側で自動的に設定するものとしてもよい。また、選択テーブル１２における暗号方式やビット長は、バージョンアップできるようにしてもよい。これにより、セキュア領域の守秘性を高めることができる。

【００６２】

（第３実施形態）

第２実施形態では、ECアプリがセキュア領域２２の使用を要求する毎に、そのECアプリに新たにパーティションをアタッチした。そうすると、セキュア領域２２の使用を要求するECアプリが増えれば、TRM１内は多くのパーティションについてのパーティションテーブルを格納せねばならず、内部EEPROM３に不足がでる。パーティションが多くなった場合、第３実施形態では、一部のパーティションについてのパーティションテーブルを外部EEPROM２内に配置する。この際、パーティションテーブルから、ECアプリに対応するパーティションが判明する恐れがあるので、暗復号化部１４はこの外部EEPROM２に置かれたパーティションテーブルは暗号化する。この際、暗復号化部１４は外部EEPROM２の他のパーティションに割り当てられたものとは異なった暗号鍵を割り当てる。

【００６３】

図１３は、本実施形態に係るパーティションテーブルのレイアウトを示す図である。本図に示すように、最後のパーティションテーブルであるパーティションテーブルnは、外部EEPROM２内に置かれている。パーティションテーブルnは、暗号化されており、その暗号鍵は、TRM１の内部EEPROM３のアプリケーション使用領域に配置されている。以降、パーティションnのアクセス時には、このパーティションテーブルnを、この暗号鍵で復号した上でなされる。

【００６４】

以上のように本実施形態によれば、他のパーティションとは異なる暗号鍵でアクセステーブルを暗号化して外部EEPROM２に格納するので、内部EEPROM３に不足が生じた場合でも、ある程度のセキュリティレベルをもったパーティションをECアプリに割り当てることができる。

尚、TRM１内のパーティションテーブルであっても外部EEPROM２内にあるパーティションテーブル同様、パーティションとは異なる暗号鍵で暗号化してもよい。

【００６５】

（第４実施形態）

Java（登録商標）仮想マシン９上で、複数ECアプリに対応するクライアントアプリが動作している場合、OS１０はこれら複数クライアントアプリを、1つのタスクとして認識してしまう。これでは、あるクライアントアプリから他のECアプリへの切り換わり時に、そのECアプリについてのデタッチを行うことができず、その切換先ECアプリが、切換元ECアプリのパーティションをアクセスすることも有り得る。

【００６６】

仮に、切換先ECアプリが悪意をもった者に操作されている場合、切換元ECアプリのパーティションの内容がその悪意をもったものに漏洩してしまう恐れがある。本実施形態では、かかる漏洩を避けるため、Java（登録商標）仮想マシン９が、クライアントアプリの切り換えがあれば、その切り換えがあった旨と、切換先APL-IDとを領域拡張部１１に通知する。

【００６７】

領域拡張部１１は、Java（登録商標）仮想マシン９からクライアントアプリの切り換えが通知されれば、ファイルシステムのデタッチを行う。

以上のように本実施形態によれば、Java（登録商標）仮想マシン９を介することにより複数タスクが1つのタスクとして認識される場合であっても、ECアプリの切り換えをJava（登録商標）仮想マシンがOS１０に通知するので、クライアントアプリのデタッチを行うことができ、あるクライアントアプリのパーティションの内容を、他のECアプリに漏洩することはない。

【００６８】

（第５実施形態）

第３実施形態では、内部EEPROM３の容量が不足した際、パーティションテーブルを外部EEPROM２に配置したが第５実施形態では、内部EEPROM３が不足したかどうかに拘らずパーティションテーブルを外部EEPROM２に配置する実施形態である。

【００６９】

外部EEPROM２に、パーティションテーブルをそのまま配置したのでは外部EEPROM２の何処に各パーティションが存在するのかが明らかである。そこで第５実施形態では、パーティションに対応するパーティションテーブルを暗号化した上で外部EEPROM２に配置しておく。この暗号化にあたっての暗号鍵は、各パーティションテーブル毎に異なるものとし、またパーティションテーブルとのパーティションとの間でも異なるものとする。

【００７０】

そしてパーティションテーブルについての暗号鍵は第４実施形態同様、内部EEPROM３に配置しておく。またパーティションのアクセスにあたっては、暗復号化部１４にパーティションテーブルの復号を行わせる。

以上のように本実施形態によれば、パーティションテーブルを内部EEPROM３ではなく暗号化した上で外部EEPROM２に配置するので、パーティションの数が多くなっても対処が可能である。

【００７１】

（第１実施形態～第５実施形態の補足事項）

(A)尚、ECアプリをアプリケーションプログラムの一例として説明したが、他のECアプリでもよい。鉄道、航空、バス、高速道路等の交通機関が運営するサーバ装置上のサーバアプリケーション、これに対応するクライアントアプリケーションであってもよい。これにより、改札業務や搭乗手続きといった用途でもSDeXメモリカードを利用することができる。

【００７２】

また、官公庁や地方公共団体が運営するサーバ装置上のサーバアプリケーション、これに対応するクライアントアプリケーションであってもよい。これにより、住民表や各種証明、登記等の用途にSDeXメモリカードを利用することができる。

(B)図１２に示したプログラムによる情報処理は、CPU、EEPROMといったハードウェア資源を用いて具体的に実現されている。つまり、プログラムと、ハードウェアとが協働した具体的手段が、使用目的に応じた情報処理を行うことにより、第１実施形態～第５実施形態に示したSDeXメモリカードは構築される。

【００７３】

プログラムによる情報処理が、ハードウェア資源を用いて具体的に実現されていることから、上記フローチャートに処理手順を示したプログラムは、自然法則を利用した技術的思想の創作と捉えることができ、プログラム単体で発明として成立する。図１２に示した処理手順は、本発明に係るプログラムの実施行為の形態を開示するものである。

【００７４】

尚、第１実施形態～第５実施形態は、SDeXメモリカードに組み込まれた態様で、本発明に係るプログラムの実施行為についての実施形態を示したが、SDeXメモリカードから分離して、第１実施形態～第５実施形態に示したプログラム単体を実施してもよい。プログラム単体の実施行為には、これらのプログラムを生産する行為(1)や、有償･無償によりプログラムを譲渡する行為(2)、貸与する行為(3)、輸入する行為(4)、双方向の電子通信回線を介して公衆に提供する行為(5)、店頭展示、カタログ勧誘、パンフレット配布により、プログラムの譲渡や貸渡を、

一般ユーザに申し出る行為(6)がある。

【００７５】

双方向の電子通信回線を介した提供行為(5)の類型には、提供者が、プログラムをユーザに送り、ユーザに使用させる行為や(プログラムダウンロードサービス)、プログラムを提供者の手元に残したまま、そのプログラムの機能のみを電子通信回線を通じて、ユーザに提供する行為(機能提供型ASPサービス)がある。

(C)図１２のフローチャートにおいて時系列に実行される各ステップの「時」の要素を、発明を特定するための必須の事項と考える。そうすると、これらのフローチャートによる処理手順は、制御方法の使用形態を開示していることがわかる。これらのフローチャートこそ、本発明に係る制御方法の使用行為についての実施形態である。各ステップの処理を、時系列に行うことで、本発明の本来の目的を達成し、作用及び効果を奏するよう、これらのフローチャートの処理を行うのであれば、本発明に係る半導体メモリカードの制御方法の実施行為に該当することはいうまでもない。

【００７６】

(D)第１実施形態～第５実施形態において耐タンパモジュール内外の不揮発メモリをEEPROMとして説明したが、不揮発メモリであればFe-RAM等他のものを採用してもよい。

(E)SDポータブルデバイス３００は、携帯電話タイプのものを一例にして説明したが、民生用の携帯オーディオ機器やSTB(Set Top Box)や携帯電話であってもよい。

【００７７】

(F)金銭に準ずるセキュアな情報として、年間の取引明細を一例にしたが、機密性が求められる情報であれば、個人情報、企業秘密情報等の他の情報であってもよい。

(G)ECアプリ固有のファイルシステム領域として領域拡張部１１は、パーティションを割り当てたが、他の論理領域をECアプリ固有のファイルシステム領域にしてもよい。例えば1つのディレクトリをECアプリ固有のファイルシステム領域にしてもよい。

【００７８】

【発明の効果】

以上説明したように本発明に係る半導体メモリカードは、耐タンパモジュールと、不揮発メモリとを備える半導体メモリカードであって、耐タンパモジュールは、内部メモリと、処理部とを含み、耐タンパモジュールの内部メモリには、アプリケーションプログラムにより利用される領域があり、前記処理部は、当該アプリケーションプログラムに固有のファイルシステム領域を不揮発メモリ上に割り当て、当該ファイルシステム領域についてのアクセステーブルを耐タンパモジュールの内部メモリ上に配置することにより、アプリケーションプログラムの利用領域の拡張を行うものである。

【００７９】

アクセステーブルを耐タンパモジュールに配置することで、マスタブートレコードーパーティションーディレクトリーファイルというファイルシステムの全体構造がどうなっているかを秘匿することができる。

不揮発メモリのうち、何処から何処までが1つのファイルシステム領域であるか、どこからどこまでが別のファイルシステム領域であるかというファイルシステム領域のアサイン解読が困難であり、ECアプリがどの領域をどのようにアクセスしているかが秘匿される。不揮発メモリにおける第３者によるファイルシステムの全体像の把握が困難であり、不正行為の糸口を与えない。

【００８０】

更に、アクセステーブルを耐タンパモジュールの内部メモリに配置することで暗号化を行わなくとも、守秘レベルを保つことができる。そのため、ファイルシステム領域をアクセスするためのオーバーヘッドがなく(つまり、アクセステーブルを暗号化するという保護ではこの暗号化がオーバヘッドとなり、処理速度の遅延要因になる)、良好な処理速度を保つことができる。

【００８１】

ここで前記処理部は、使用領域の拡張にあたって、拡張領域を利用するアプリケーションプログラムに固有の暗号鍵を割り当て(1)、アプリケーションプログラムが前記拡張領域にデータを書き込もうとする際、当該データを暗号化し(2)

、アプリケーションプログラムが当該拡張領域からデータを読み出そうとする際、当該データを復号化する(3)暗復号化部を備えてもよい。

【００８２】

ECアプリに固有の暗号鍵を割り当てた上で、ファイルシステム領域の読み書きをECアプリに行わせる。半導体メモリカードが複数ECアプリによりアクセスされ、そのうち1つのECアプリが自身に割り当てられた暗号鍵を暴露したとしても、他のECアプリが半導体メモリカードに書き込んだデータは、その暗号鍵では復号化しえない。1つのECアプリにおける暗号鍵暴露の影響を、他のECアプリに波及させないので、ECアプリが半導体メモリカードに書き込んだデータの守秘性を高めることができる。

【００８３】

ここで前記処理部は、アプリケーションプログラムからセキュリティレベルを受け付ける受付部と、セキュリティレベルがとり得る複数の値と、それらの値に対応する暗号鍵のビット長、暗号方式を記憶する記憶部とを備え、前記暗復号化部により割り当てられる暗号鍵は、受付手段が受け付けたセキュリティレベルに対応するビット長に基づき生成され、前記暗復号化部による暗号化及び復号化は、受付手段が受け付けたセキュリティレベルに対応する暗号方式に基づきなされてもよい。

【００８４】

ECアプリはデータの読み書きにあたって、データの重要性と、そのデータの読み書きに費やする処理とからセキュリティレベルを設定して、そのセキュリティレベルに基づく、データ読み書きを半導体メモリカードの処理部に求めることができる。そのためデータサイズが大きく、重要度が低いデータは、セキュリティレベルを低く設定してデータ書き込みが短期間に終了するよう、ユーザに配慮することができる。

【００８５】

ここで前記処理部は、別のアプリケーションプログラムの利用領域の拡張を、不揮発メモリ上に別のアプリケーションプログラムについてのファイルシステム領域を割り当て、同不揮発メモリ上に当該ファイルシステム領域についてのアク

セステーブルを配置することにより行い、前記暗復号化部は、ファイルシステム領域とは異なる暗号鍵をアクセステーブルに割り当てて、その暗号鍵で、アクセステーブルを暗号化した上で不揮発メモリ上に配置しても良い。耐タンパモジュールにおける内部メモリの容量が小さく、複数ファイルシステム領域のうち何れかのファイルシステム領域テーブルが内部メモリに格納しえない場合でもECアプリに固有のファイルシステム領域を割り当てることが可能になる。

【図面の簡単な説明】

【図１】　SDeXメモリカードの使用環境を示す図である。

【図２】　本発明にかかる半導体メモリカードの内部構成を示す図である。

【図３】　TRM１内のハードウェア構成を示す図である。

【図４】　図３のTRM１内のマスクROM６とCPU７とからなる部分を、ソフトウェア構成に置き換えて描いた図である。

【図５】　外部EEPROM２及び内部EEPROM３の論理フォーマットを示す図である。

【図６】　セキュア領域２２、認証領域２３、非認証領域２４の内部構成を示す図である。

【図７】　パーティションの共通構成を示す図である。

【図８】

（ａ）　パーティションテーブルを示す図である。

（ｂ）　図７のパーティション内のパーティションブートセクタを示す図である。

【図９】　ECサーバ１００によるSDeXメモリカードのアクセス、SDポータブルデバイス３００によるSDeXメモリカードのアクセスを示す図である。

【図１０】　SDeXメモリカード、SDポータブルデバイス３００、ECサーバ１００間におけるコマンド･レスポンスのシーケンス図である。

【図１１】　第２実施形態に係るOS１０の内部構成を示す図である。

【図１２】

（ａ）　領域拡張部１１及び暗復号化部１４の処理手順を示すフローチャートである。

（ｂ）　領域拡張部１１及び暗復号化部１４によるファイル書き込みの処理手順を示すフローチャートである。

（ｃ）　領域拡張部１１及び暗復号化部１４によるファイル読み出しの処理手順を示すフローチャートである。

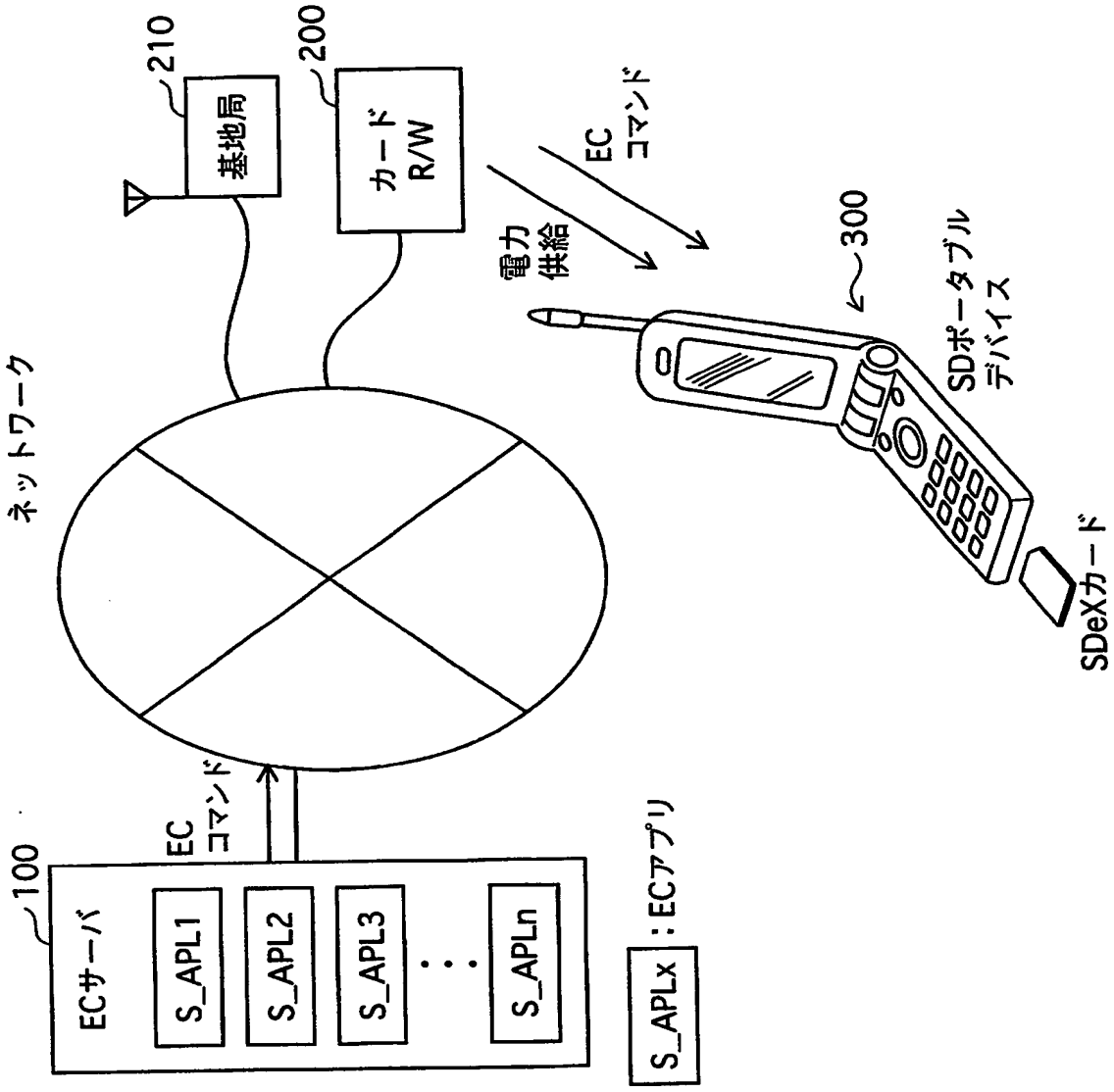
【図１３】　第２実施形態に係るパーティションテーブルのレイアウトを示す図である。

【符号の説明】

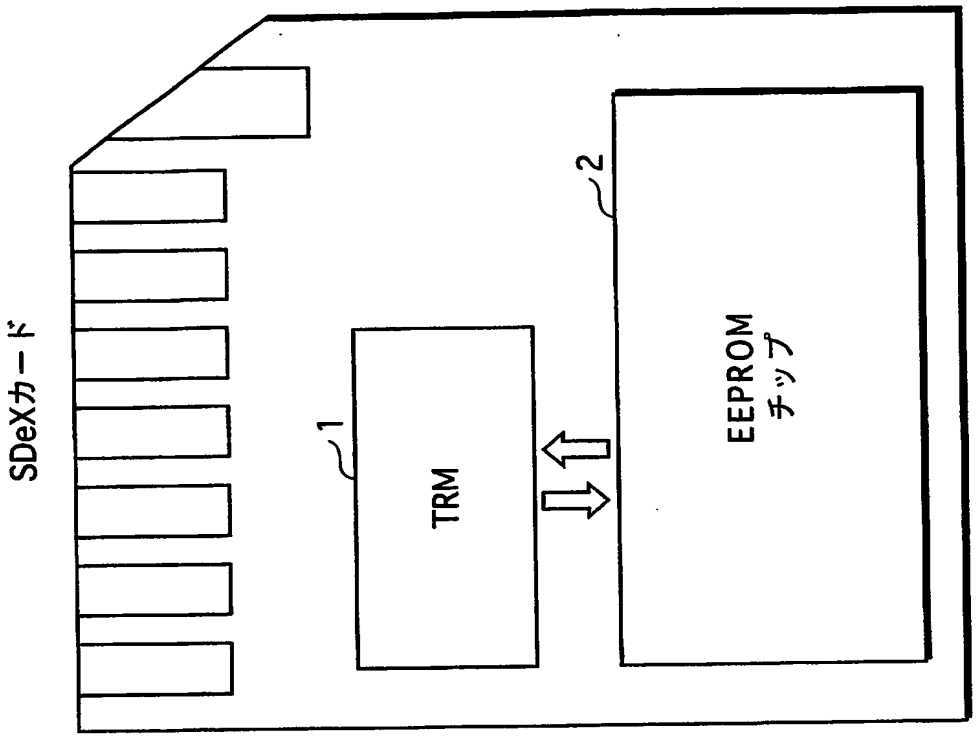
１	TRM
２	外部EEPROM
３	内部EEPROM
４	外部メモリアクセス部
５	HIM
６	マスクROM
７	CPU
８	クライアントアプリ
９	仮想マシン
１０	OS
１１	領域拡張部
１２	選択テーブル
１３	暗号化テーブル
１４	暗復号化部
２１	ECアプリの使用領域
２２	セキュア領域
２３	認証領域
２４	非認証領域
１００	ECサーバ
２００	カードリーダライタ
２１０	無線基地局
３００	SDポータブルデバイス

【書類名】　図面

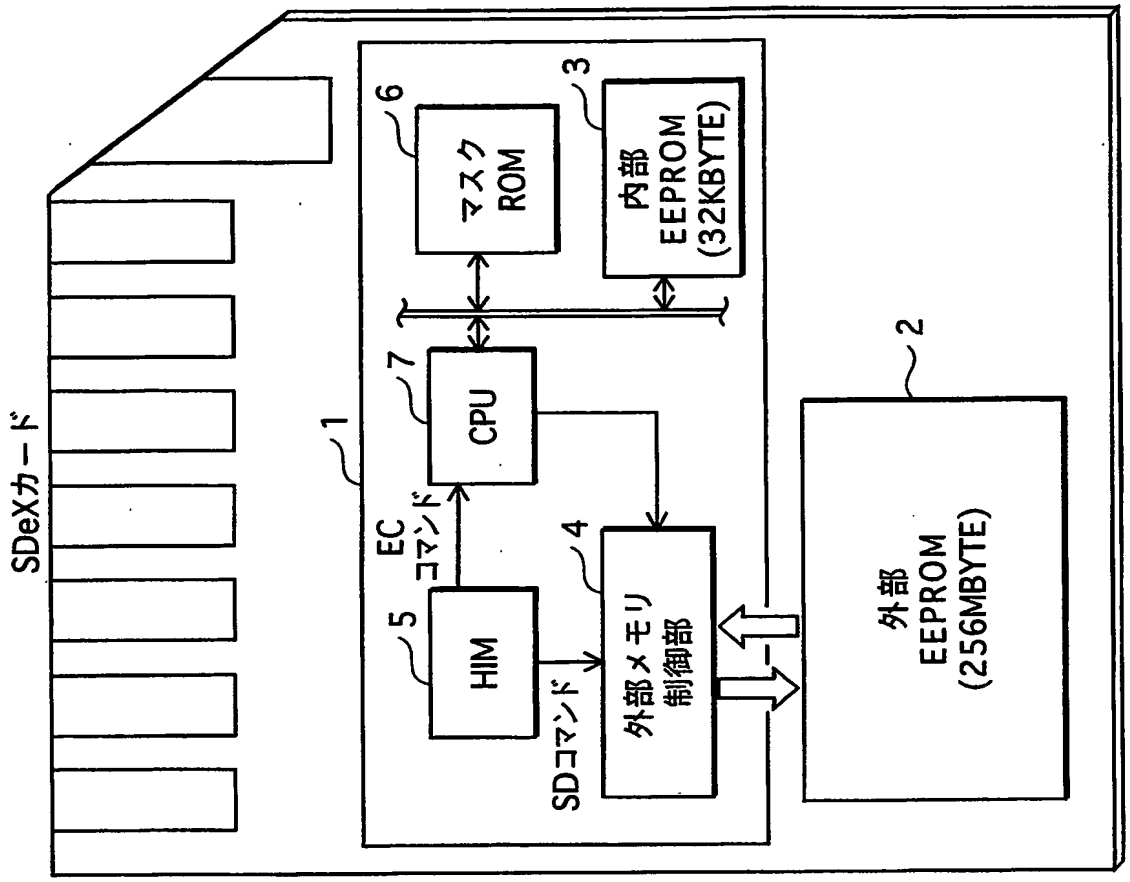
【図１】


210
基地局
200
カード
R/W
EC
コマンド
電力
供給
300
SDポータブル
デバイス
SDeXカード
ネットワーク
EC
コマンド
100
ECサーバ
S_APL1
S_APL2
S_APL3
S_APLn
S_APLx
:ECアプリ

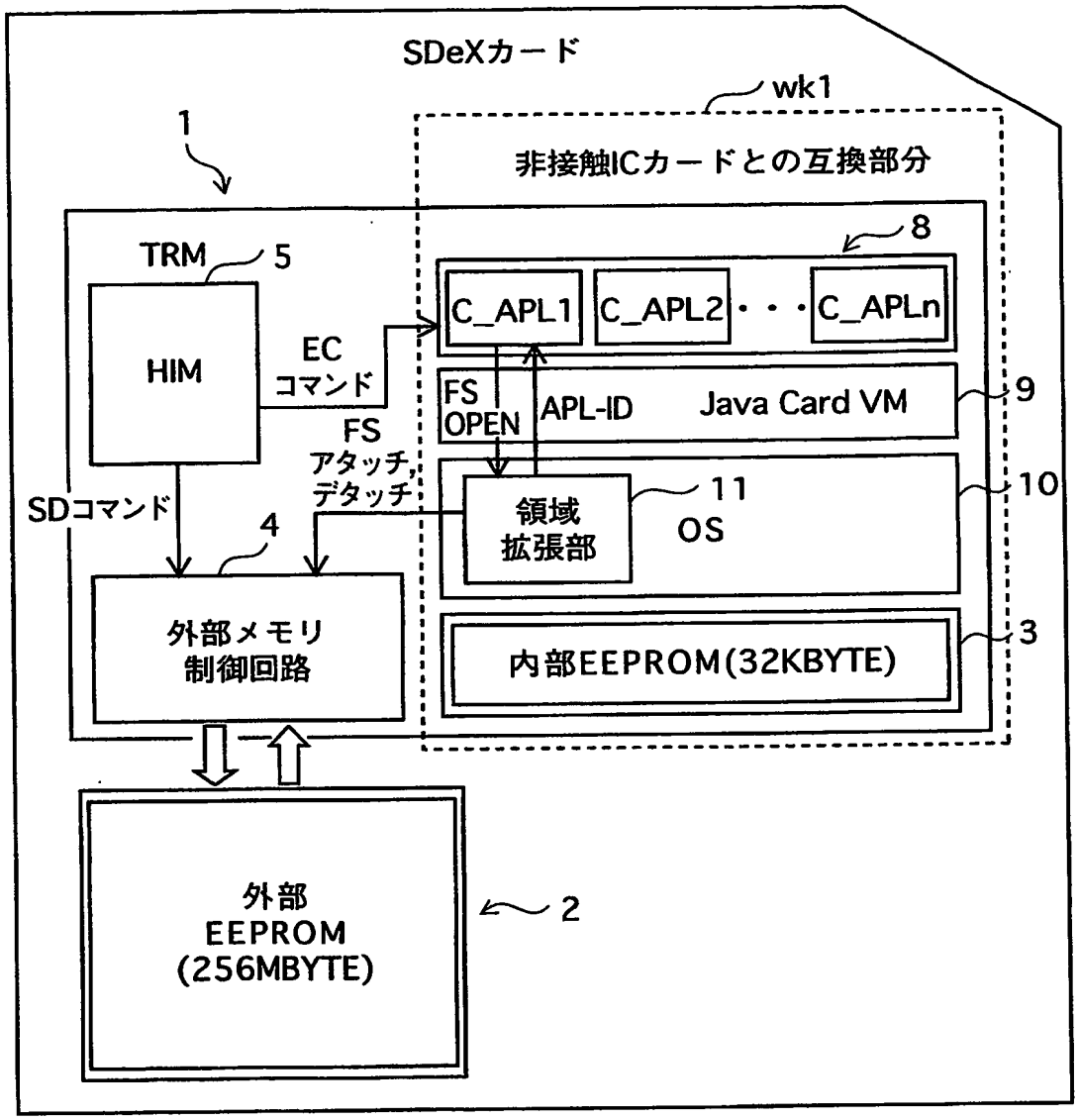
【図２】



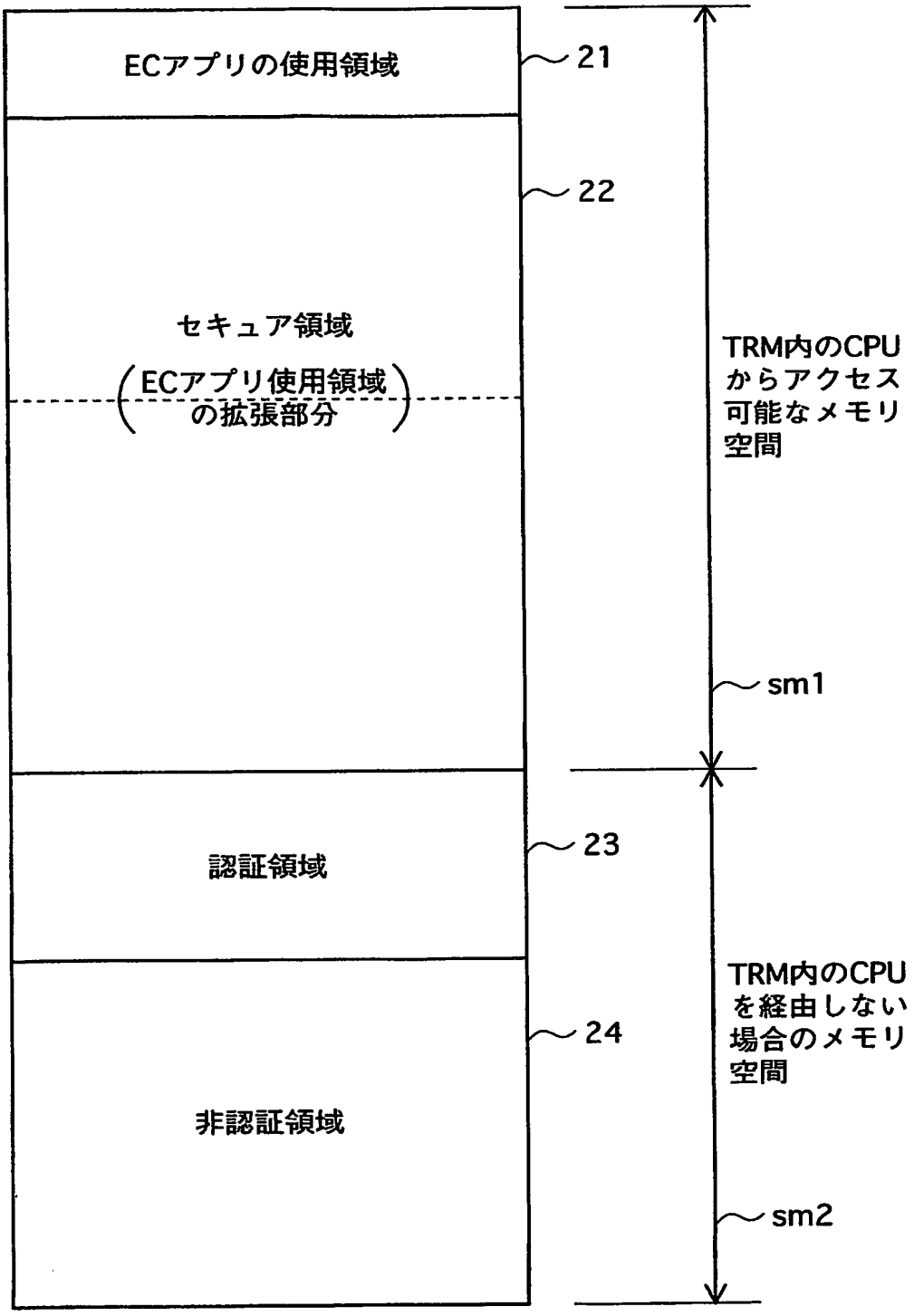
【図３】


SDeXカード
1
マスク ROM
6
内部 EEPROM (32KBYTE)
3
CPU
7
EC コマンド
HIM
5
外部メモリ制御部
4
SDコマンド
外部 EEPROM (256MBYTE)
2

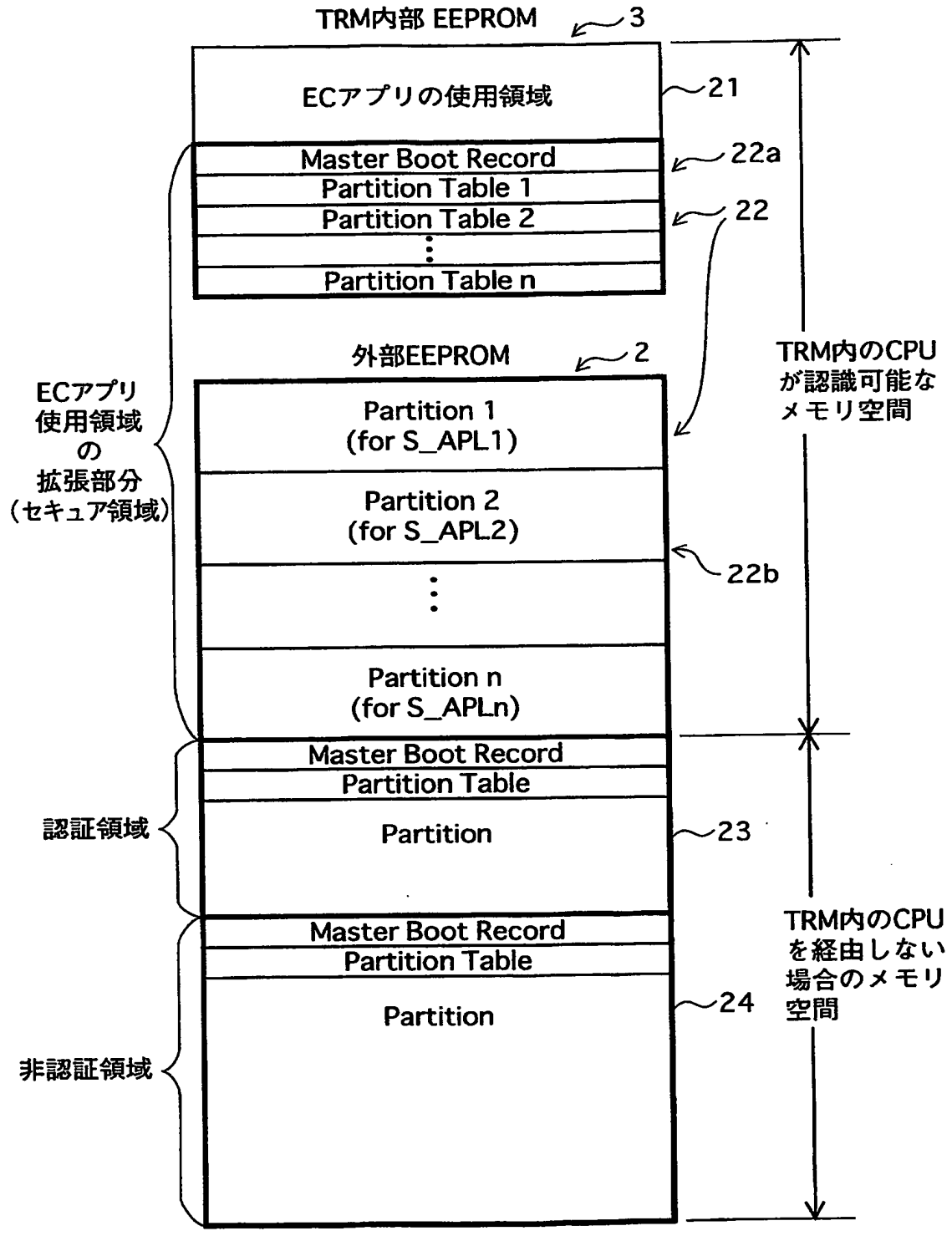
【図４】


SDeXカード
wk1
1
非接触ICカードとの互換部分
8
TRM
5
HIM
EC
コマンド
C_APL1
C_APL2
・・・
C_APLn
FS
OPEN
APL-ID
Java Card VM
9
FS
アタッチ,
デタッチ
SDコマンド
4
領域
拡張部
11
OS
10
外部メモリ
制御回路
内部EEPROM(32KBYTE)
3
外部
EEPROM
(256MBYTE)
2

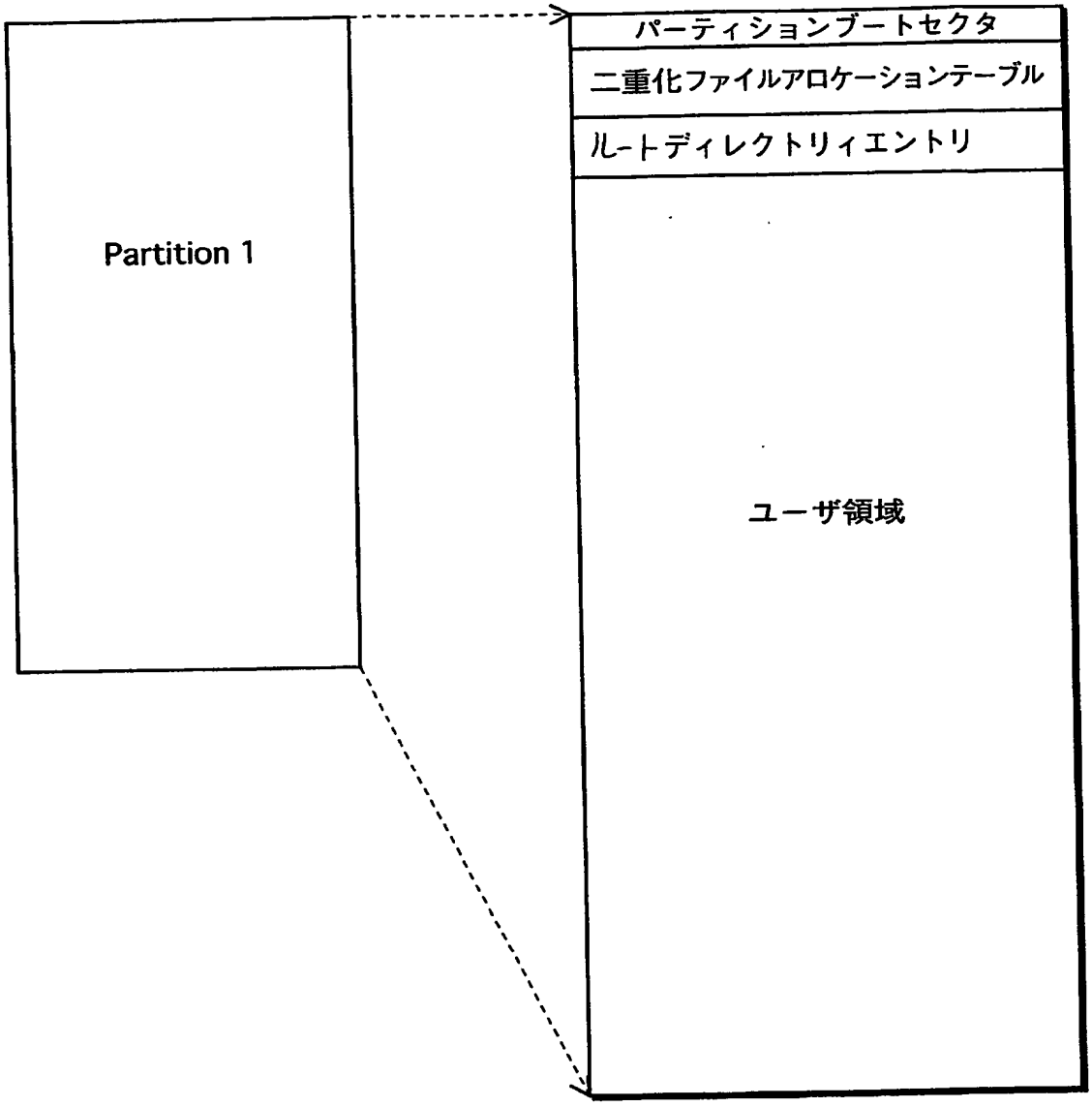
【図５】


ECアプリの使用領域
21
22
セキュア領域
(ECアプリ使用領域の拡張部分)
TRM内のCPUからアクセス可能なメモリ空間
sm1
認証領域
23
TRM内のCPUを経由しない場合のメモリ空間
24
非認証領域
sm2

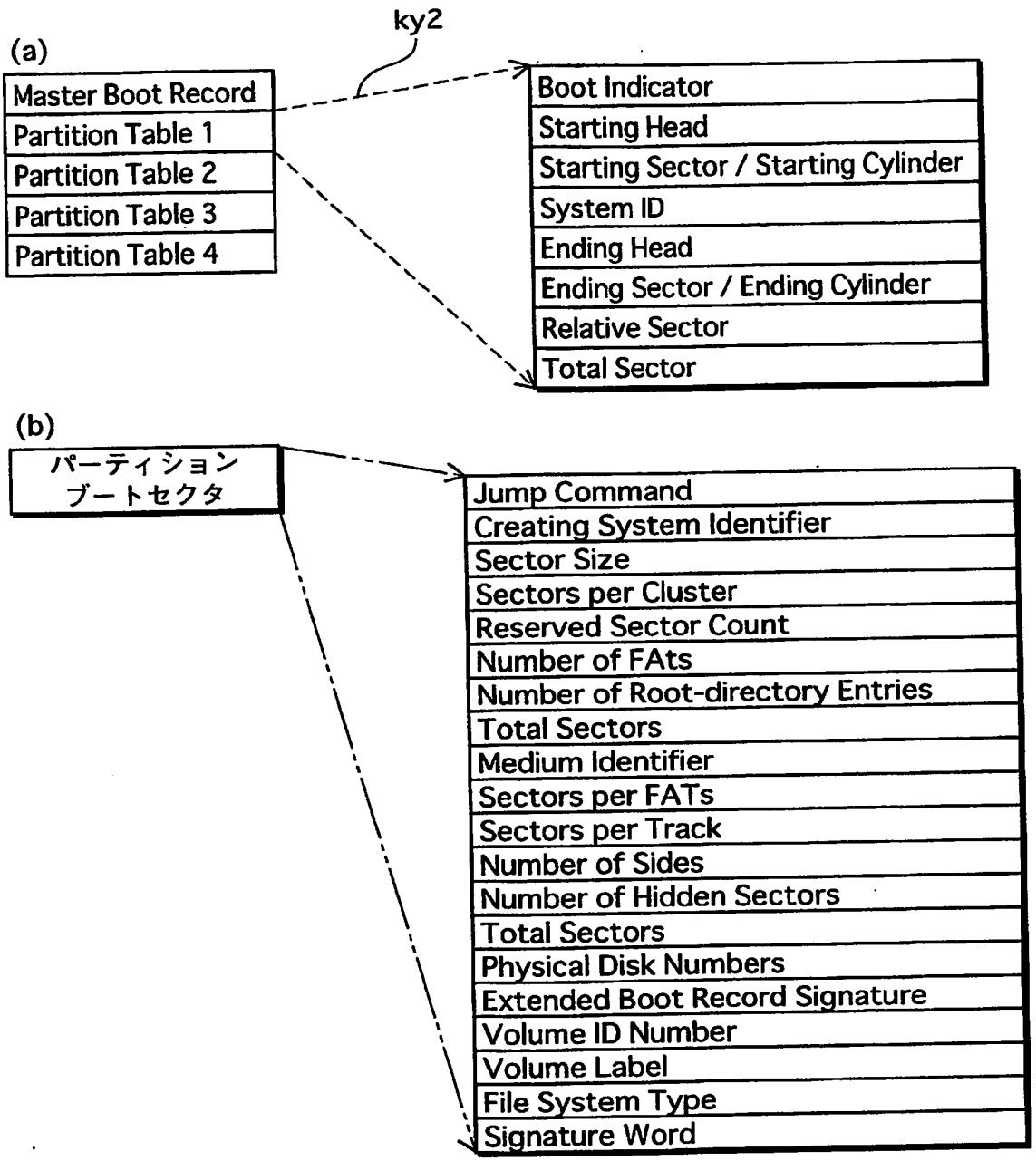
【図６】


TRM内部 EEPROM
3
ECアプリの使用領域
21
Master Boot Record
Partition Table 1
Partition Table 2
Partition Table n
22a
22
外部EEPROM
2
Partition 1
(for S_APL1)
Partition 2
(for S_APL2)
Partition n
(for S_APLn)
22b
Master Boot Record
Partition Table
Partition
23
Master Boot Record
Partition Table
Partition
24
ECアプリ
使用領域
の
拡張部分
（セキュア領域）
認証領域
非認証領域
TRM内のCPU
が認識可能な
メモリ空間
TRM内のCPU
を経由しない
場合のメモリ
空間

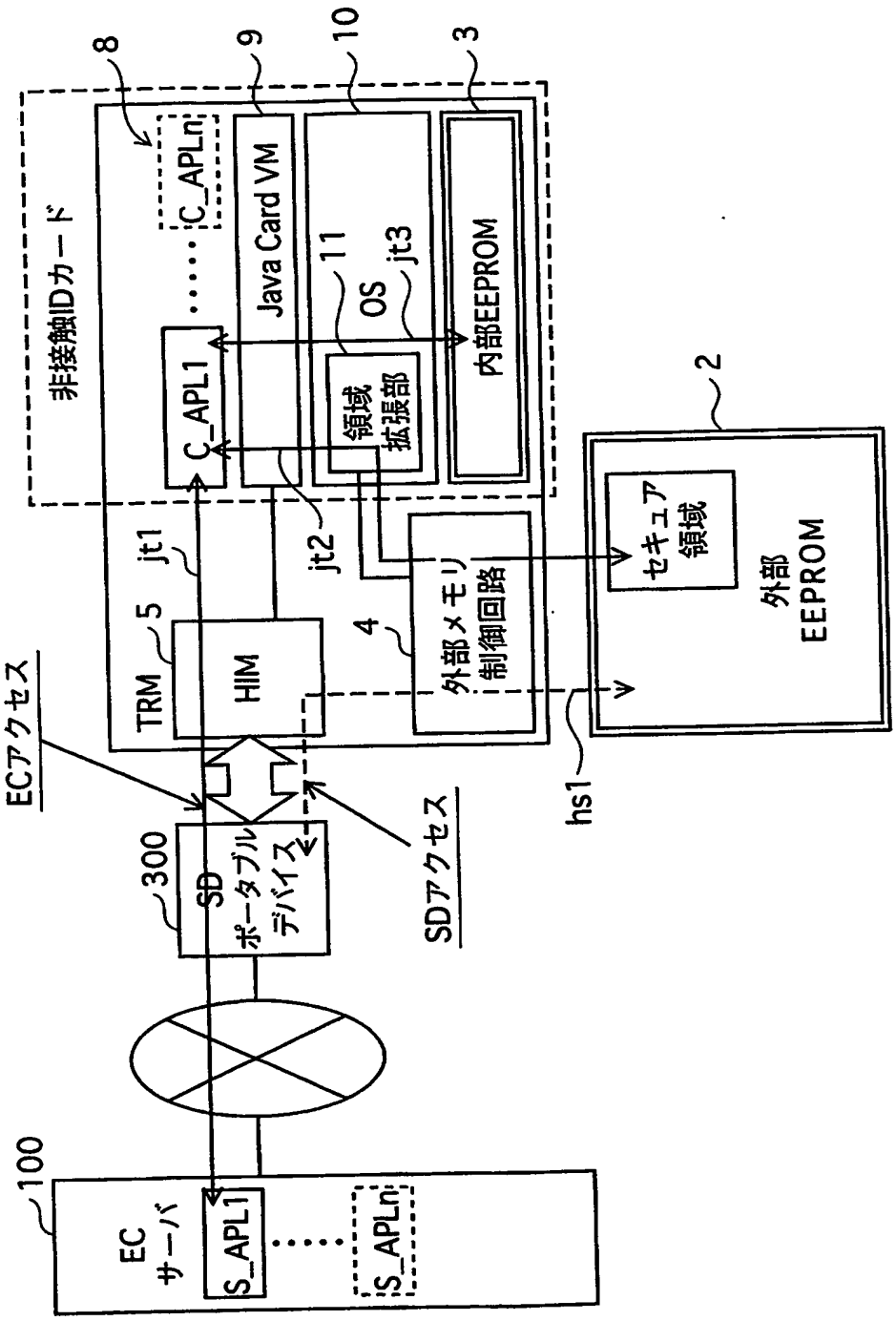
【図７】


Partition 1
パーティションブートセクタ
二重化ファイルアロケーションテーブル
ルートディレクトリィエントリ
ユーザ領域

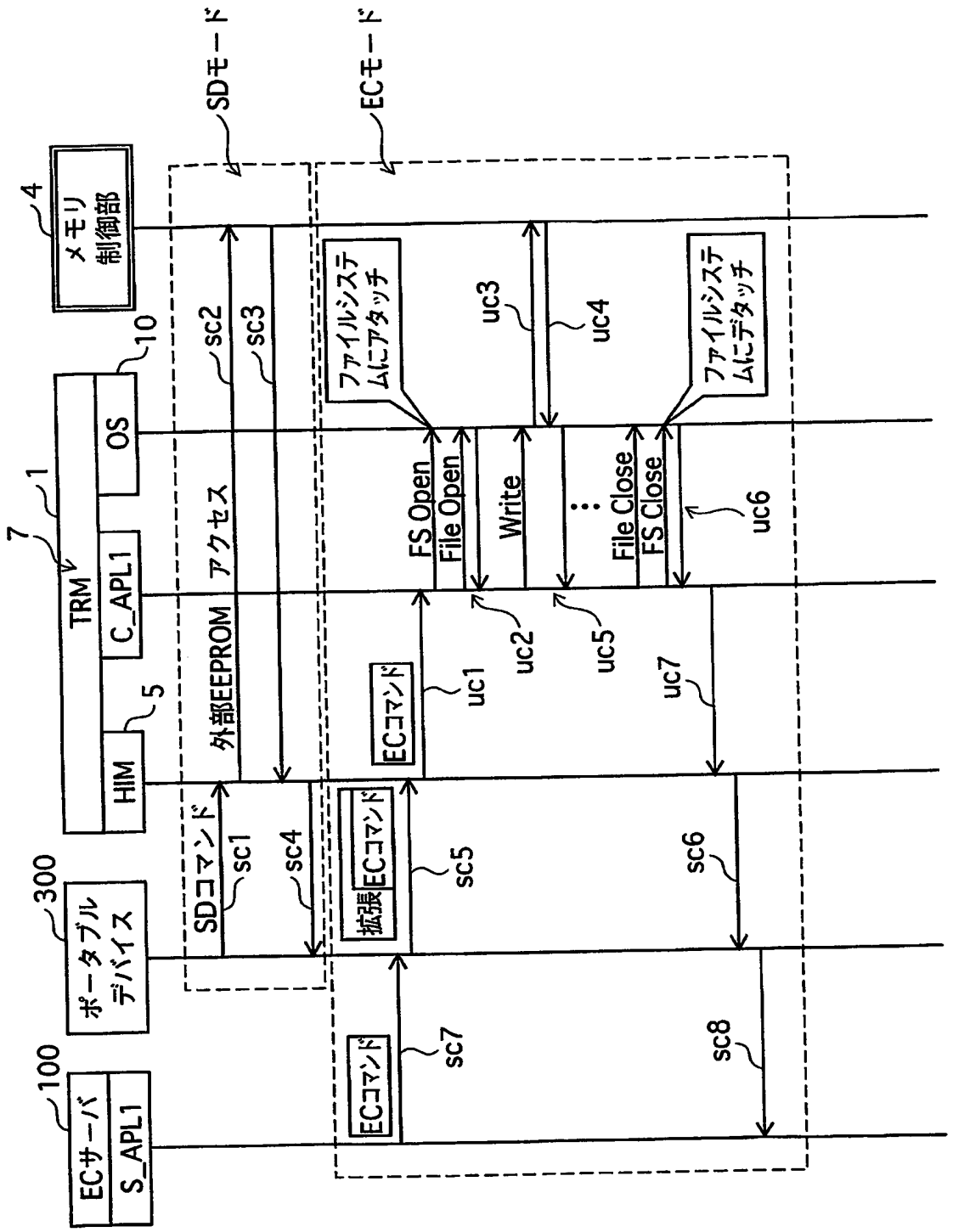
【図８】


(a)
ky2
Master Boot Record
Partition Table 1
Partition Table 2
Partition Table 3
Partition Table 4
Boot Indicator
Starting Head
Starting Sector / Starting Cylinder
System ID
Ending Head
Ending Sector / Ending Cylinder
Relative Sector
Total Sector
(b)
パーティション
ブートセクタ
Jump Command
Creating System Identifier
Sector Size
Sectors per Cluster
Reserved Sector Count
Number of FATs
Number of Root-directory Entries
Total Sectors
Medium Identifier
Sectors per FATs
Sectors per Track
Number of Sides
Number of Hidden Sectors
Total Sectors
Physical Disk Numbers
Extended Boot Record Signature
Volume ID Number
Volume Label
File System Type
Signature Word

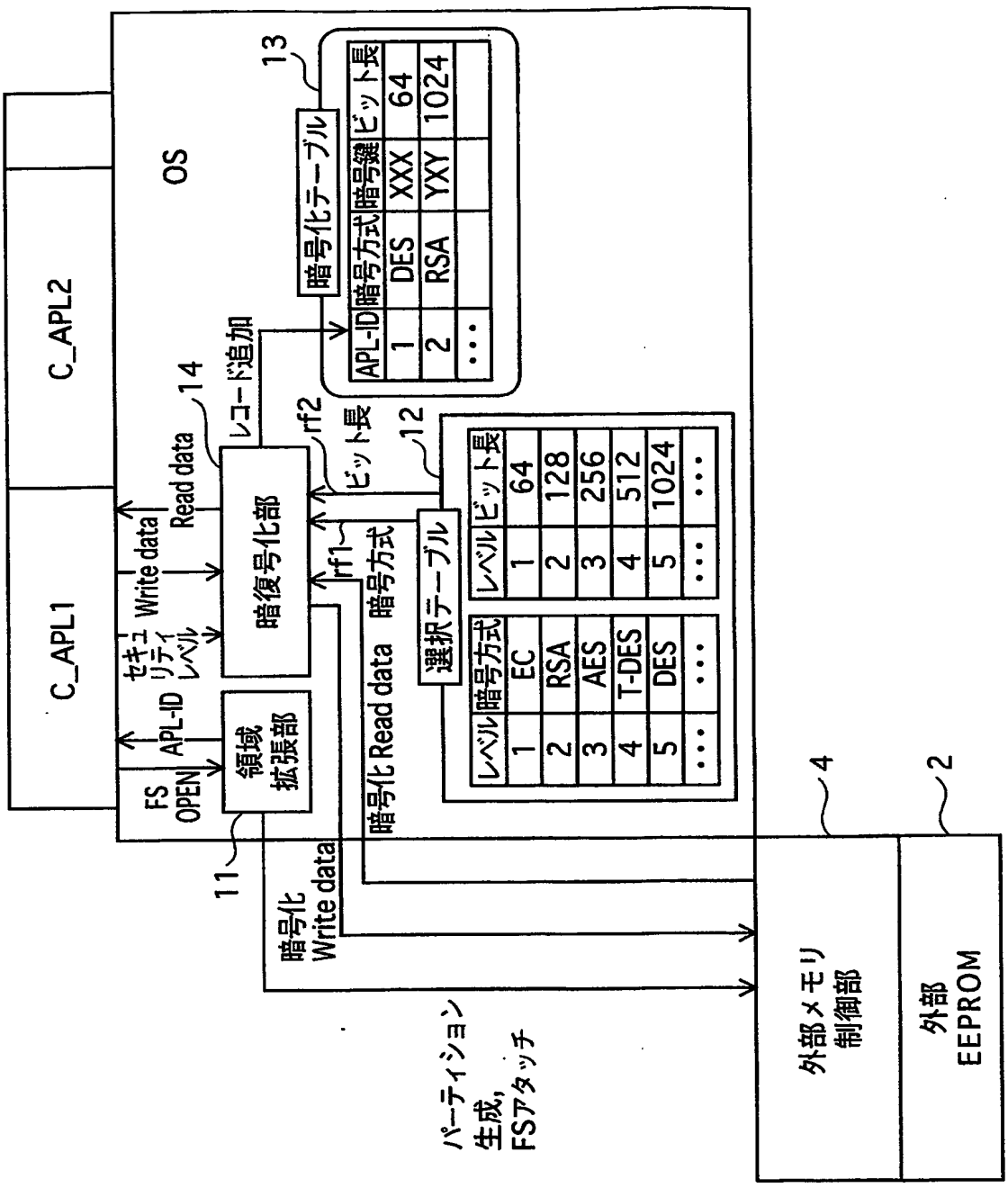
【図９】


非接触IDカード
8
9
10
3
C_APLn
C_APL1
Java Card VM
11
OS
jt3
領域
拡張部
内部EEPROM
2
セキュア
領域
外部
EEPROM
jt1
jt2
5
TRM
HIM
4
外部メモリ
制御回路
hs1
ECアクセス
SDアクセス
300
SD
ポータブル
デバイス
100
EC
サーバ
S_APL1
S_APLn

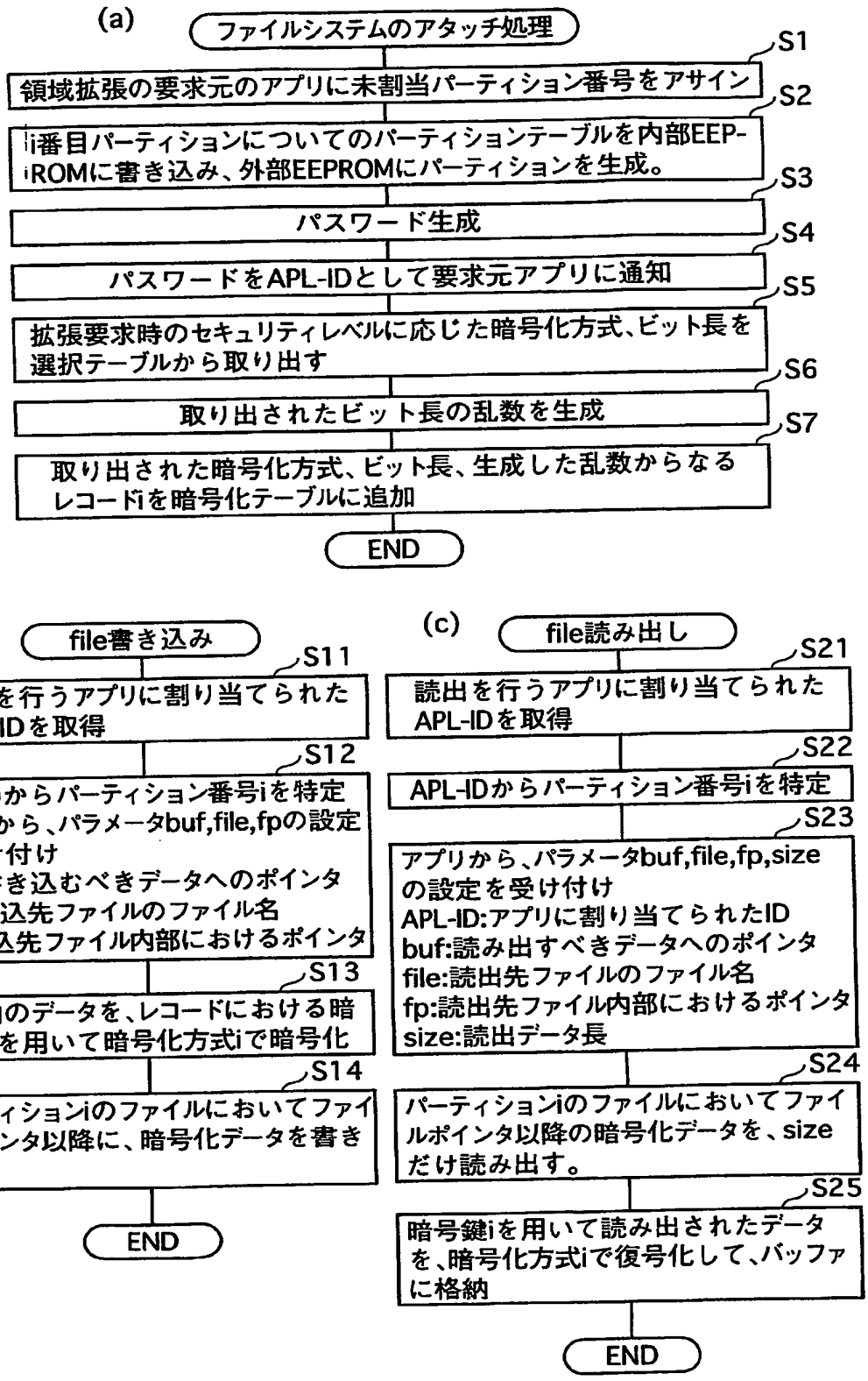
【図１０】


SDモード
ECモード
4
メモリ制御部
10
OS
1
7
TRM
C_APL1
5
HIM
外部EEPROM
アクセス
sc2
sc3
ファイルシステムにアタッチ
uc3
uc4
ファイルシステムにデタッチ
FS Open
File Open
Write
File Close
FS Close
uc6
uc1
uc2
uc5
uc7
ECコマンド
300
ポータブルデバイス
SDコマンド
sc1
sc4
拡張ECコマンド
sc5
sc6
100
ECサーバ
S_APL1
ECコマンド
sc7
sc8

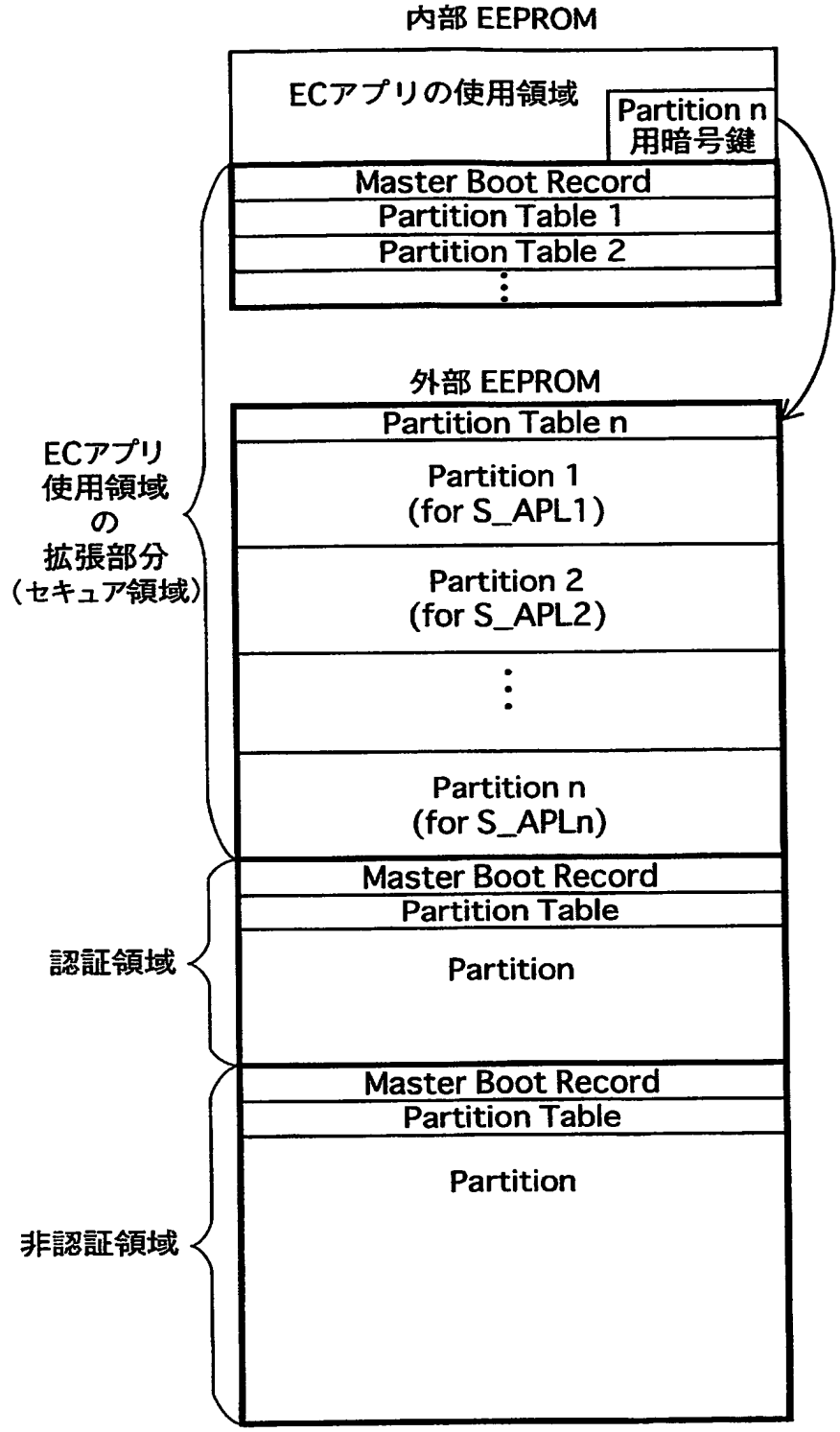
【図１１】


C_APL1
C_APL2
OS
FS OPEN
APL-ID
セキュリティレベル
Write data
Read data
領域拡張部
暗復号化部
レコード追加
rf1
rf2
ビット長
暗号方式
選択テーブル
暗号化テーブル
APL-ID
暗号方式
暗号鍵
ビット長
1 DES XXX 64
2 RSA YXY 1024
レベル
暗号方式
1 EC
2 RSA
3 AES
4 T-DES
5 DES
レベル
ビット長
1 64
2 128
3 256
4 512
5 1024
暗号化 Read data
暗号化 Write data
パーティション生成，FSアタッチ
外部メモリ制御部
外部EEPROM
11
12
13
14
4
2

【図１２】


(a)
ファイルシステムのアタッチ処理
S1
領域拡張の要求元のアプリに未割当パーティション番号をアサイン
S2
i番目パーティションについてのパーティションテーブルを内部EEP-iROMに書き込み、外部EEPROMにパーティションを生成。
S3
パスワード生成
S4
パスワードをAPL-IDとして要求元アプリに通知
S5
拡張要求時のセキュリティレベルに応じた暗号化方式、ビット長を選択テーブルから取り出す
S6
取り出されたビット長の乱数を生成
S7
取り出された暗号化方式、ビット長、生成した乱数からなるレコードiを暗号化テーブルに追加
END
(b)
file書き込み
S11
書込を行うアプリに割り当てられたAPL-IDを取得
S12
APL-IDからパーティション番号iを特定
アプリから、パラメータbuf,file,fpの設定を受け付け
buf:書き込むべきデータへのポインタ
file:書込先ファイルのファイル名
fp:書込先ファイル内部におけるポインタ
S13
buf内のデータを、レコードにおける暗号鍵iを用いて暗号化方式iで暗号化
S14
パーティションiのファイルにおいてファイルポインタ以降に、暗号化データを書き込む
END
(c)
file読み出し
S21
読出を行うアプリに割り当てられたAPL-IDを取得
S22
APL-IDからパーティション番号iを特定
S23
アプリから、パラメータbuf,file,fp,sizeの設定を受け付け
APL-ID:アプリに割り当てられたID
buf:読み出すべきデータへのポインタ
file:読出先ファイルのファイル名
fp:読出先ファイル内部におけるポインタ
size:読出データ長
S24
パーティションiのファイルにおいてファイルポインタ以降の暗号化データを、sizeだけ読み出す。
S25
暗号鍵iを用いて読み出されたデータを、暗号化方式iで復号化して、バッファに格納
END

【図１３】


内部 EEPROM
ECアプリの使用領域
Partition n
用暗号鍵
Master Boot Record
Partition Table 1
Partition Table 2
外部 EEPROM
Partition Table n
Partition 1
(for S_APL1)
Partition 2
(for S_APL2)
Partition n
(for S_APLn)
ECアプリ
使用領域
の
拡張部分
（セキュア領域）
Master Boot Record
Partition Table
Partition
認証領域
Master Boot Record
Partition Table
Partition
非認証領域

【書類名】　要約書

【課題】　ECアプリがデータを書き込もうとする際、容量が不足することのない半導体メモリカードを提供する。

【解決手段】　TRM１内部のEEPROM３にあるECアプリの使用領域を拡張する。この拡張は、内部EEPROM３内にパーティションテーブルを配置しつつ、TRM１外部EEPROM２にパーティションを生成してECアプリに割り当てるというものである。パーティションテーブルがTRM１内にあるので、生成されたパーティションテーブルは、TRM１内のCPU７からしかアクセスできない。拡張領域に対するアクセスが、TRM１内のCPU７に限られるので、格納内容の守秘性が高まる。

【選択図】　図３

特願２００３－０２４１６７

出願人履歴情報

識別番号 [０００００５８２１]

１．変更年月日 １９９０年 ８月２８日
[変更理由] 新規登録
住所 大阪府門真市大字門真１００６番地
氏名 松下電器産業株式会社